November 2012

Glossary

of SECURITY TERMS, DEFINITIONS, and ACRONYMS

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Table of Contents

Glossary Terms 04

A 05
B 20
C 24
D 68
E 94
F 105
G 122
H 126
I 129
J 146
K 147
L 148
M 153
N 160
O 171
P 180
Q 200
R 201
S 212
T 239
U 252
V 260
W 263

Note: To return to the TOC, click the button at the bottom left of each glossary page

Acronym Terms 266

A 267
B 270
C 272
D 281
E 287
F 290
G 293
H 294
I 295
J 300
K 301
L 301
M 303
N 306
O 313
P 316
Q 320
R 320
S 322
T 329
U 333
V 335
W 335
X 336
Y 336

Note: To return to the TOC, click the button at the bottom left of each acronym page

Glossary Terms

Acceptable Level of Risk
An authority's determination of the level of potential harm to an operation, program, or activity that the authority is willing to accept due to the loss of information.

Access
The ability and opportunity to obtain knowledge of classified information.

Access requires formal indoctrination and execution of a non-disclosure agreement.

Access Approval
Formal authorization for an individual to have access to classified or sensitive information within a Special Access Program (SAP) or a Controlled Access Program (CAP), including Sensitive Compartmented Information (SCI).

Access Approval Authority (AAA)
Individual responsible for final access approval and/or denial determination.

Access Control
A procedure to identify and/or admit personnel with proper security clearance and required access approval(s) to information or facilities using physical, electronic, and/or human controls.

Access Control Mechanisms
Measures or procedures designed to prevent unauthorized access to protected information or facilities.

Access Eligibility Determination
A formal determination that a person meets the personnel security requirements for access to a specified type or types of classified information.

Access Evaluation
The process of reviewing the security qualifications of employees.

Access National Agency Check with Inquiries (ANACI)
A personnel security investigation for access to classified information conducted by the Office of Personnel Management (OPM), combining a national agency check and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools, and a credit check.

ANACIs are only conducted on civilian employees and do not apply to military or contractor personnel.

Access Roster
A database or listing of individuals briefed to a Special Access Program (SAP).

Access Termination
The removal of an individual from access to Special Access Program (SAP) or other program information.

Accesses
Indoctrination to classified material that has additional security requirements or caveats. This may be Sensitive Compartmented Information

(SCI), Special Access Program (SAP) information, or collateral level accesses (North Atlantic Treaty Organization (NATO) or Critical Nuclear Weapons Design Information (CNWDI)).

Accessioned Records
Records of permanent historical value in the legal custody of National Archives and Records Administration (NARA).

Accountability
Assignment of a document control number, including copy number (#), which is used to establish individual responsibility for the document and permits traceability and disposition of the document.

Accreditation
The formal certification by a Cognizant Security Authority (CSA) that a facility, designated area, or information system has met Director of National Intelligence (DNI) security standards for handling, processing, discussing, disseminating or storing Sensitive Compartmented Information (SCI).

Accreditation (of Information Systems (IS))
The approval to use an Information System (IS) to process classified information in a specified environment at an acceptable level of risk based upon technical, managerial, and procedural safeguards.

Accredited Security Parameter (ASP)
The security classification levels, compartments, and sub-compartments at which an Information

System (IS) or network is accredited to operate (e.g., TOP SECRET or Special Access Required (SAR)).

Accrediting Authority
A customer official who has the authority to decide on accepting the security safeguards prescribed or who is responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Acknowledged Special Access Program
A Special Access Program (SAP) that is acknowledged to exist and whose purpose is identified (e.g., the B-2 or F-117 aircraft program) while the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is generally unclassified.

NOTE: Members of the four Congressional Defense Committees are authorized access to the program.

Acoustical Intelligence
Intelligence information derived from the collection and analysis of acoustical phenomena.

Acoustical Security
Those security measures designed and used to deny aural access to classified information.

Acquisition Program
A directed, funded effort that provides a new, improved, or continuing materiel, weapon,

Information System (IS), or service capability in response to an approved need.

Acquisition Special Access Program
A Special Access Program (SAP) established primarily to protect sensitive research, development, testing, and evaluation or procurement activities in support of sensitive military and intelligence requirements.

Acquisition Systems Protection
The safeguarding of defense systems anywhere in the acquisition process as defined in Department of Defense Directive (DoDD) 5000.1, "The Defense Acquisition System," the defense technologies being developed that could lead to weapon or defense systems and defense research data. Acquisition Systems Protection integrates all security disciplines, counterintelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our forces uncompromised combat effectiveness over the life expectancy of the system.

Activity
A Department of Defense (DoD) unit, organization, or installation performing a function or mission.

Activity Security Manager (ASM)
The individual specifically designated in writing and responsible for the activity's information security program which ensures that classified and Controlled Unclassified Information (CUI)

is properly handled during its entire life cycle. This includes ensuring classified information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken.

The Activity Security Manager (ASM) may be assigned responsibilities in other security disciplines, such as personnel or physical security.

Adjudication
Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information, and continue to hold positions requiring a trustworthiness decision.

Adjudication Authority
Entity which provides adjudication for eligibility or access.

Adjudicative Process
An examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk.

Adjudicator
A personnel security specialist who performs adjudications.

Adversary
An individual, group, organization, or Government

that must be denied Critical Program Information (CPI). Synonymous with competitor/enemy.

Adversary Collection Methodology
Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

Adversary Threat Strategy
The process of defining, in narrative or graphical format, the threat presented to an operation, program, or project.

The adversary threat strategy should define the potential adversaries, the courses of action those adversaries might take against the operation, and the information needed by the adversaries to execute those actions.

Adverse Action
A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction of pay, or furlough of 30 days or less.

Adverse Information
Any information that adversely reflects on the integrity or character of a cleared employee that suggests his or her ability to safeguard classified information may be impaired, or that his or her access to classified information may not clearly be in the interest of national security.

Affiliate
Any entity effectively owned or controlled by another entity.

Agency
Any executive agency as defined in 5 United States Code (U.S.C.) 105, "Executive Agency," and any other entity within the executive branch that comes into the possession of classified information.

Agent
A person who engages in a clandestine activity.

Agent of the Government
A contractor employee designated in writing by the Government Contracting Officer who is authorized to act on behalf of the Government.

Alien
Any person who is not a citizen of the United States (U.S.).

Alternative Compensatory Control Measures
Used to safeguard sensitive intelligence or operations and support information (acquisition programs do not qualify) when normal measures are insufficient to achieve strict Need-to-Know controls, and where Special Access Program (SAP) controls are not required.

Analysis
The process by which information is examined in order to identify significant facts and/or derive conclusions.

Anti-Tamper
Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

Anti-Tamper Executive Agent (ATEA)
The Department of Defense (DoD) Anti-Tamper Executive Agent (ATEA), chartered by the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)), and assigned to the Directorate for Special Programs, Office of the Assistant Secretary of the Air Force for Acquisition.

Appeal
A formal request under the provisions of Executive Order (EO) 12968, Section 5.2, "Access to Classified Information," for review of a denial or revocation of access eligibility.

Applicant
A person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

Application
Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

Approved Access Control Device
Any access control device that meets the requirements of Department of Defense Manual (DoDM) 5220.22-M as approved by the Facility Security Officer (FSO).

Approved Built-in Combination Lock
A combination lock, equipped with a top-reading dial that conforms to Underwriters' Laboratories, Inc. Standard Number, UL 768, Group IR.

Approved Combination Padlock
A three-position dial-type changeable combination padlock listed on the Government Services Administration (GSA) Qualified Products List as meeting the requirements of Federal Specification FF-P-110.

Approved Electronic, Mechanical, or Electro-Mechanical Device
An electronic, mechanical, or electro-mechanical device that meets the requirements of Department of Defense Manual (DoDM) 5220.22-M as approved by the Facility Security Officer (FSO).

Approved Key-Operated Padlock
A padlock which meets the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number (NSN) 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), NSN 5340-00-799-8016.

Approved Security Container
A security file container, originally procured from a Federal Supply Schedule (FSS) supplier, that

conforms to Federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock.

Such containers will be labeled "General Services Administration Approved Security Container" on the face of the top drawer.

Acceptable tests of these containers can be performed only by a testing facility specifically approved by the General Services Administration (GSA).

Approved Vault
A vault constructed in accordance with Department of Defense Manual (DoD) 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," and approved by the Cognizant Security Agency (CSA).

Approved Vault Door
A vault door and frame unit originally procured from the Federal Supply Schedule (FSS), Group 71, Part III, Section E, FSS, Class 7110, that meets Federal Specification AA-D-600.

Assessment
To evaluate the worth, significance, or status of something; especially to give an expert judgment of the value or merit of something.

Asset
Any resource—a person, group, relationship, instrument installation, or supply—at the disposition

of an intelligence agency for use in an operational or support role.

A person who contributes to a clandestine mission but is not a fully controlled agent.

Associated (Enhanced) Markings
Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "classified by" line, downgrading and declassification instructions, special control notices, and Special Access Program (SAP) caveats, etc.

Astragal Strip
A narrow strip of material applied over the gap between a pair of doors for protection from unauthorized entry and sound attenuation.

See: Sound Attenuation

Authentication
Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authenticity
Having an undisputed identity or origin.

Authorized Adjudicative Agency
An agency authorized by law or regulation, or direction of the Director of National Intelligence (DNI) to determine eligibility for access to classified information in accordance with Executive Order

(EO) 12698, "Adjustments of Certain Rates of Pay and Allowances."

Authorized Classification and Control Markings Register
The official list of authorized security control markings and abbreviated forms of such markings for use by all elements of the Intelligence Community (IC) for classified and unclassified information.

Also known as the Controlled Access Program Coordination Office (CAPCO) Register.

Authorized Investigative Agency
Any agency authorized by law, executive order, regulation or the Director, Office of Management and Budget (OMB) under Executive Order (EO) 13381, "Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information," to conduct Counterintelligence (CI) investigations or investigations of persons who are proposed for access to sensitive or classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

Authorized Person
A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement (NdA), and has a Need-to-Know (NTK) for the specific classified information in the performance of official duties.

Authorized User (AU)
Any appropriately cleared individual with a requirement to access a Department of Defense (DoD) Information System (IS) in order to perform or assist in a lawful and authorized Governmental function.

Automated Information System (AIS)
A generic term applied to all electronic computing systems. Automated Information Systems (AIS) collect, store, process, create, disseminate, communicate, or control data or information.

AIS are composed of computer hardware (e.g., automated data processing equipment and associated devices that may include communication equipment), firmware, an operating system (OS), and other applicable software.

Automated Information System Media Control System
A system of procedures approved by the Program Security Officer (PSO), which provide controls over use, possession, and movement of magnetic media in a Special Access Program Facility (SAPF).

The procedures must ensure all magnetic media (classified and unclassified) are adequately protected to avert the unauthorized use, duplication, or removal of the media. The media must be secured in limited access containers or labeled with the identity of the individual responsible for maintaining the material.

Automatic Declassification
The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority (OCA), or the expiration of a maximum time frame for duration of classification established under this order.

Availability
Timely, reliable access to data and information services for authorized users as defined in Department of Defense (DoD) 8500.1, Information Assurance (IA).

Background Investigation (BI)
A personnel security investigation consisting of both record reviews and interviews with sources of information covering the most recent 5 years of an individual's life, or since the 18th birthday, whichever is shorter, provided that at least 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Balanced Magnetic Switch
A type of intrusion detection system sensor which may be installed on any rigid, operable opening (e.g., doors or windows) through which access may be gained to the Special Access Program Facility (SAPF) and Sensitive Compartmented Information (SCI).

Bank Secrecy Act (BSA)
Also known as the Currency and Foreign Transactions Reporting Act, the Bank Secrecy Act (BSA) of 1970 was enacted to reduce the amount of secrecy in the banking system by requiring financial institutions to help identify activities that may amount to money laundering.

See: Financial Crimes Enforcement Network (FINCEN)

Beta I
Security Certification testing performed in a lab environment or other facility, as appropriate.

Beta II
Security Certification testing performed at designated operational installations(s) until a

stable baseline is achieved.

NOTE: Configuration differences or other factors may necessitate multiple Beta II test sites.

Billets

A determination that in order to meet Need-to-Know criteria, certain Special Access Programs (SAPs) may elect to limit access to a predetermined number of properly cleared employees.

Security personnel do not count against the billet system.

BLACK

A designation applied to telecommunications and Information Systems (IS), including associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.

BLACK Equipment

A term applied to equipment that processes only unclassified and/or encrypted information.

BLACK Line

An optical fiber or a metallic wire that carries a BLACK signal or that originates/terminates in a BLACK equipment or system.

BLACK Optical Fiber Line

An optical fiber that carries a BLACK signal or that originates/terminates in a BLACK equipment or system.

BLACK Wire Line
A metallic wire that carries a BLACK signal or that originates/terminates in a BLACK equipment or system.

Boundary
The boundary of an Automated Information System (AIS) or network includes all users that are directly or indirectly connected and who can receive data from the system without a reliable human review by an appropriately cleared authority.

Break-Wire Detector
An Intrusion Detection System (IDS) sensor used with screens and grids, open wiring, and grooved stripping in various arrays and configurations necessary to detect surreptitious and forcible penetrations of movable openings, floors, walls, ceilings, and skylights. An alarm is activated when the wire is broken.

Burn Bag
The informal name given to a container (usually a paper bag or some other waste receptacle) that holds sensitive or classified documents which are to be destroyed by fire or pulping after a certain period of time.

The most common usage of burn bags is by Government institutions, in the destruction of materials deemed classified.

Burn-In

A tendency for an image that is shown on a display over a long period of time to become permanently fixed on the display.

This is most often seen in emissive displays such as Cathode Ray Tube and Plasma as chemical change can occur in the phosphors when exposed repeatedly to the same electrical signals.

BUSTER

A computer program that is part of the Computer Security Tool-box.

BUSTER is a Microsoft Disk Operating System (MS-DOS)-based program used to perform a binary search of a disk or diskette for any word or set of words found in a search definition file by performing a linear search on a disk or diskette, four sectors at a time.

BUSTER uses the "LIMITS.TXT" file as it documents search word patterns.

Camouflage
The use of natural or artificial material on personnel, objects, or positions (e.g., tactical) in order to confuse, mislead, or evade the enemy/ adversary.

Carve-Out
A classified contract for which the Defense Security Service (DSS) has been relieved of inspection responsibility in whole or in part.

Case Officer
A professional employee of an intelligence organization who is responsible for providing direction for an agent operation.

See: Camouflage; Concealment; Deception

Case-by-Case Basis
The principle that a disclosure authorization is restricted to individual events or occasions to prevent confusion with permanent and repetitive disclosure determinations.

Caveat
A designator used with or without a security classification to further limit the dissemination of restricted information (e.g., For Official Use Only (FOUO) and Not Releasable to Foreign Nationals (NOFORN)).

Central Adjudication Facility (CAF)
A single facility designated by the head of the Department of Defense (DoD) component to evaluate personnel security investigations and other relevant information.

Central United States Registry for North Atlantic Treaty Organization (NATO)
The North Atlantic Treaty Organization (NATO) controls its classified records through a registry system in which individual documents are numbered and listed in inventories.

The Central United States Registry is located in Arlington, Virginia, and oversees more than 125 sub-registries domestically and abroad.

Certification
A statement to an accrediting authority of the extent to which an Automated Information System (AIS) or network meets its security criteria.

A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process.

Certification and Accreditation (C&A)
The standard Department of Defense (DoD) approach for identifying information security requirements, providing security solutions, and managing the security of DoD Information Systems (IS).

See: Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)

Certified Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Technical Authority (CTTA)
A United States (U.S) Government employee who has met established certification requirements in accordance with the Committee on the National

Security Systems (CNSS)-approved criteria and has been appointed by a United States Government department or agency to fulfill Certified Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Technical Authority (CTTA) responsibilities.

Character Investigation (CI)
An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to character and reliability.

Civil Service Commission (CSC)
The United States (U.S.) Civil Service Commission (CSC) was created by the Pendleton Civil Service Reform Act in 1883 to administer the civil service of the Federal Government.

In 1978, the functions of the CSC were split between the Office of Personnel Management (OPM) and the Merit Systems Protection Board (MSPB), with additional functions placed under the purview of the Equal Employment Opportunity Commission (EEOC), the Federal Labor Relations Authority (FLRA) and the Office of Special Counsel (OSC).

Classification
The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Official information that has been determined, pursuant to EO 12958 or a predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated.

See: Classified Information

Classification and Control Markings (CCM)
The Controlled Access Program Coordination Office (CAPCO) uses a uniform list of security classification and control markings that are compiled in the Authorized Classification and Control Marking Register.

There are nine general categories of classification and control markings:

1. United States (U.S.) Classification
2. Non-U.S. Classification
3. Joint Classification
4. Sensitive Compartmented Information (SCI) Control Systems
5. Special Access Program (SAP) Markings
6. Foreign Government Information (FGI) Markings
7. Dissemination Controls
8. Non-Intelligence Community Markings
9. Document Declassification

See: Classification and Control Markings System (Intelligence Community Directive (ICD) 710)

Classification and Control Markings System (Intelligence Community Directive (ICD) 710)
A companion document to the Authorized Classification and Control Marking Register that provides guidance on the syntax and use of classification and control markings. Intelligence Community Directive (ICD) 710, "Classification and Control Markings System," establishes the Intelligence Community (IC) classification and control markings system as a critical element of IC procedures for protecting intelligence and information.
See: Classification and Control Markings (CCM)

Classification Guidance
Any instruction or source that prescribes the classification of specific information.

Classification Guide
A documentary form of classification guidance issued by an Original Classification Authority (OCA) that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. A classification guide is created for any system, program, policy, or project under the cognizance of the OCA.

Classification Levels
Information may be classified at one of the following three levels:

- TOP SECRET: Security classification that shall

be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

- SECRET: Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- CONFIDENTIAL: Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Classification Markings and Implementation Working Group (CMIWG)

An Intelligence Community (IC) forum under the purview of the Director of National Intelligence (DNI) Classification and Control Markings (CCM) branch.

The Classification Markings and Implementation Working Group (CMIWG), comprised of IC and non-IC members, are responsible for coordinating changes to the Controlled Access Program Coordination Office (CAPCO) Authorized

Classification and Control Markings Register and associated implementation manual.

Classified Contract
Any contract that requires access to classified information, by a contractor or his or her employees. A contract may be a classified contract even though the contract document is not classified.

The requirements for a classified contract also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Agency (GCA) programs or projects which require access to classified information by a contractor.

Classified Information
As defined by the Classified Information Procedures Act (CIPA) of 1980, classified information is defined as official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.
See: Classified Information Procedures Act (CIPA)

Classified Information Procedures Act (CIPA)
The Classified Information Procedures Act (CIPA), passed by Congress in 1980, defines classified information as any information or material that has been determined by the United States (U.S.) Government pursuant to an executive order, statute, or regulation, to require protection against

unauthorized disclosure for reasons of national security and any restricted data, as defined in Paragraph R of Section 11 of the Atomic Energy Act (AEA) of 1954 (42 U.S.C. 2014[y]).

See: Classified Information

Classified Military Information (CMI)
Information originated by or for the Department of Defense (DoD) or its agencies, or is under their jurisdiction or control, and that requires protection in the interests of national security.

It is designated TOP SECRET, SECRET, or CONFIDENTIAL. Classified Military Information (CMI) may be conveyed via oral, visual, or material form.

Classified National Security Information (CNSI)
Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order (EO) 13526, "Classified National Security Information."

See: Classified Information

Classified Visit
A visit during which a visitor will require, or is expected to require, access to classified information.

Classifier
Any person who makes a classification determination and applies a classification category to information or material. The

determination may be an original classification action or it may be a derivative classification action.

Contractors make derivative classification determinations based on classified source material, a security classification guide, or a Contract Security Classification Specification (CSCS).

Clearance
An administrative authorization for access to National Security Information (NSI) up to a stated classification level (TOP SECRET, SECRET, CONFIDENTIAL).

Clearance Certification
An official notification that an individual holds a specific level of security clearance and/or access approval(s), authorizing the recipient of the certification access to classified information or materials at that level.

Cleared Commercial Carrier
A carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program (NISP).

Cleared Employees
All contractor employees granted personnel security clearances (PCLs) and all employees being processed for PCLs.

See: Clearance; Security Clearance, Personnel Security Clearance

Cleared Escort
An appropriately cleared United States (U.S.) citizen, at least 18 years old, who performs access control/escort duties on limited and minor construction, repair or maintenance projects in Sensitive Compartmented Information Facilities (SCIFs) or other classified areas that do not require a Construction Surveillance Technician.

Clearing
The removal of information from the media to facilitate continued use and to prevent the Automated Information System (AIS) from recovering previously stored data. However, the data may be recovered using laboratory techniques.

Overwriting and degaussing are acceptable methods of clearing media.

Closed Area
An area that meets the requirements of Intelligence Community Directive (ICD) 705, "Sensitive Compartmented Information Facilities," for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Per the NISPOM, a closed area is one that meets NISPOM requirements for safeguarding classified

information that because of its size, nature, or operational necessity, cannot be adequately protected by normal safeguards or stored during nonworking hours in approved containers.

Closed Storage
The storage of Special Access Program (SAP) and Sensitive Compartmented Information (SCI) material in properly secured General Services Administration (GSA)-approved security containers within an accredited Special Access Program Facility (SAPF).

Coalition
An arrangement between one or more nations for common action. The multi-national relationship results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members, usually for single occasions or longer cooperation in a narrow sector of common interest.

A force composed of military elements of nations that have formed a temporary alliance for some specific purpose.

Code Word
A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation.

Codec A
Set of equipment that encodes an analogue speech or video signal into digital form for

transmission purposes and at the receiving end decodes the digital signal into a form close to its original form.

Coercive Force
A negative or reverse magnetic force applied for the purpose of reducing magnetic flux density (demagnetization).
See: Coercivity

Coercivity
A property of magnetic material, measured in Oersteds (Oe) or Amperes per meter units (A/M), used as a measure of the amount of coercive force required to reduce the magnetic induction to zero from its remnant state (demagnetization).

Generally used as a measure of the difficulty with which magnetic Information System (IS) storage devices can be degaussed.
See: Coercive Force

Cognizant Security Agency (CSA)
Agencies of the Executive Branch that have been authorized by Executive Order (EO) 12829, "National Industrial Security Program (NISP)," to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry.

These agencies include the Department of Defense (DoD), Department of Energy (DOE), Central Intelligence Agency (CIA), and Nuclear Regulatory Commission (NRC).

Cognizant Security Authority (CSA)
The single principal designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods and is under SOIC responsibility.

Cognizant Security Office (CSO)
The organizational entity delegated by the Head of a Cognizant Security Agency (CSA) to administer industrial security on behalf of the CSA.

Cohabitant
Individuals living together in a spouse-like relationship, including the mutual assumption of those marital rights, duties and obligations which are usually manifested by married people, including, but not necessarily dependent on, sexual relations.

Collateral Effect
Unintentional or incidental effects including, but not limited to, injury or damage to persons or objects that would not be lawful military targets under the circumstances ruling at the time. Includes effects on civilian or dual-use computers, networks, information, or infrastructure.

Such effects are not unlawful as long as they are not excessive in light of the overall military advantage anticipated from the activity.

In cyberspace operations, collateral effects are categorized as:

- High: Substantial adverse effects on persons or property that are not lawful targets from which there is a reasonable probability of loss of life, serious injury, or serious adverse effect on the affected nation's security, economic security, public safety, or any combination of such effects.
- Medium: Substantial adverse effects on persons or property that are not lawful targets.
- Low: Temporary, minimal, or intermittent effects on persons or property that are not lawful targets.
- No: Only adversaries and their computers, computer-controlled networks, information, and information systems are adversely affected.

Collateral Information
All National Security Information (NSI) classified CONFIDENTIAL, SECRET, or TOP SECRET under the provisions of an executive order for which special community systems of compartmentation (e.g., non-Special Compartmented Information (non-SCI)) are not formally established.

Command and Control Warfare (C2W)
The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction.

Command and Control Warfare (C2W) is mutually supported by intelligence to deny information

to, influence, degrade, or destroy adversary command and control capabilities. This process is accomplished while protecting friendly command and control capabilities against such actions.

C2W applies across the operational continuum and all levels of conflict.

Command Authority
The individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Commercial and Government Entity (CAGE) Code
A Commercial and Government Entity (CAGE) Code is a five position code that identifies companies doing or wishing to do business with the Federal Government. The first and fifth positions in the code must be numeric. The third and fourth positions may be any mixture of alpha/numeric excluding I and O. The code is used to support a variety of mechanized systems throughout the Government.

Commercial Off-The-Shelf (COTS)
A term for software or hardware, generally technology or computer products, that are ready-made and available for sale, lease, or license to the general public. Commercial off-the-Shelf (COTS) products are often used as alternatives to in-house developments or one-off Government-funded developments.

The use of COTS products is being mandated

across many Government and business programs, as they may offer significant savings in procurement and maintenance. However, since COTS software specifications are written by external sources, Government agencies are sometimes wary of these products because they fear that future changes to the product will not be under their control.

Common Operational Picture (COP)
A continuously updated overview of an incident compiled throughout an incident's lifecycle from data shared between integrated systems for communication, information management, and intelligence and information sharing.

The common operational picture (COP) also helps ensure consistency at all levels of incident management across jurisdictions, as well as between various Governmental jurisdictions and private sector and non-Governmental entities that are engaged.

Common Wall Facility
A facility that shares a building wall, floor, or ceiling with uninspectable areas.

Communications Intelligence
Technical and intelligence information derived from the intercept of foreign communications by other than the intended recipients of those communications.

Communications Profile
An analytic model of communications associated

with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the Communications Security (COMSEC) measures applied.

Communications Security (COMSEC)
Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications.

COMSEC includes cryptosecurity, transmission security, emission security, and physical security of classified material.

Communications Security Monitoring
The act of listening to, copying, or recording transmissions of one's own official telecommunications in order to analyze the degree of security.

Community of Interest (COI)
A restricted network of users, each having an Information System (IS) with an accredited security parameter identical to the others, and the need to communicate securely with other members of the network.

Community Risk
Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

Company
A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to carry out a commercial, industrial or other legitimate business, enterprise, or undertaking.

Compartmentation
A formal system for restricting access to selected activities or information. The establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties.

Compartmented Intelligence
National intelligence placed in a Director of National Intelligence (DNI)-approved control system to ensure handling by specifically identified access approved individuals.

Compelling Need
A requirement for immediate access to special program information to prevent failure of the mission or operation or other cogent reasons.

Compromise
Unauthorized intentional or unintentional disclosure of information or data to unauthorized persons. Compromise is also a security policy violation of a

system in which, modification, destruction, or loss of an object may have occurred.

Compromising Emanations (CE)
Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

Computer Network
The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

Computer Network Attack (CNA)
A category of "fires" employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems and networks themselves. The ultimate intended effect is not necessarily on the target system itself, but may support a larger effort, such as information operations or counterterrorism (e.g., altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels).

NOTE: The term "fires" means the use of weapon systems to create specific lethal or nonlethal effects on a target.

See: Computer Network Exploitation (CNE); Cyber Operational Preparation of the Environment (C-OPE)

Computer Network Exploitation (CNE)
Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated information systems or networks.

See: Computer Network Attack (CNA); Cyber Operational Preparation of the Environment (C-OPE)

Computer Security
Measures and controls that ensure confidentiality, integrity, and availability of information systems assets, including hardware, software, firmware, and information being processed, stored, and communicated.

Computer Security Act
The Computer Security Act of 1987, Public Law (PL) No. 100-235 (H.R. 145), was enacted by Congress on January 8, 1988 to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems.

The act requires the creation of computer security plans and the appropriate training of system

users or owners where the systems house sensitive information.

NOTE: The Computer Security Act has been superseded by the Federal Information Security Management Act (FISMA) of 2002.

See: Federal Information Security Management Act (FISMA)

Computer Security Toolbox
A set of tools (e.g., BUSTER, FLUSH, and Secure Copy) designed specifically to assist Information Assurance Officers (IAOs) and System Administrators (SAs) in performing their duties.

The functions within the Toolbox can erase appended data within files; eliminate appended data in free or unallocated space; search for specific words or sets of words for verifying classification; and locate unapproved share programs. It also includes a program which allows you to clear laser toner cartridges and drums.

See: BUSTER; FLUSH

Computerized Telephone System (CTS)
A generic term used to describe any telephone system that uses centralized stored program computer technology to provide switched telephone networking features and services.

CTSs are commercially referred to by such terms as Computerized Private Branch Exchange (CPBX), Private Branch Exchange (PBX), Private Automatic Branch Exchange (PABX), Electronic Private Automatic Branch Exchange

(EABX), Computerized Branch Exchange (CBX), Computerized Key Telephone Systems (CKTS), hybrid key systems, business communications systems, and office communications systems.

Computing Environment
Workstation or server (host) and its Operating System (OS), peripherals, and applications.

Concealment
The act of remaining hidden.

Concept of Intelligence Operations
A verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations.

The concept of intelligence operations, which supports the commander's concept of operations, is contained in the intelligence annex of operation plans.

The concept of intelligence operations is designed to give an overall picture of intelligence support for joint operations. It is included primarily for additional clarity of purpose.

See: Concept of Operations (CONOPS)

Concept of Operations (CONOPS)
A verbal or graphic statement that clearly and concisely expresses what the force commander intends to accomplish and how it will be done using available resources.

Condition (Personnel Security)
Access eligibility granted or continued with the

proviso that one or more additional measures will be required. Such measures include additional security monitoring, restrictions on access, and restrictions on an individual's handling of classified information. Submission of periodic financial statements, admonishment regarding use of drugs or excessive use of alcohol, and satisfactory progress in a Government-approved counseling program is examples of conditions.

See: Exception (Personnel Security); Deviation (Personnel Security); Waiver (Personnel Security)

CONFIDENTIAL
The designation applied to information or material of which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

Confidential Source
Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States (U.S.) on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Confidentiality
An assurance that information is not disclosed to unauthorized entities or processes.

Configuration Control
Process of controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against

improper modifications prior to, during, and after system implementation.

See: Configuration Management (CM)

Configuration Management (CM)
A discipline applying technical and administrative direction and surveillance to:

1. Identify and document the functional and physical characteristics of a configuration item
2. Control changes to those characteristics
3. Record and report changes to processing and implementation status

Connection Approval
Formal authorization to interconnect Information Systems (IS).

Connectivity
Indicates the connection of two systems regardless of the method used physical connection.

Consignee
A person, firm, or Government activity names as the receiver of a shipment; one to whom a shipment is consigned.

Consignor
A person, firm, or Government activity by which articles are shipped. The consignor is usually the shipper.

Constant Surveillance Service
A transportation protective service provided by a commercial carrier qualified by Surface Deployment and Distribution Command (SDDC)

to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative. A Facility Security Clearance (FCL), however, is not required for the carrier.

The carrier providing the service must maintain a signature and tally record for the shipment.

See: Surface Deployment and Distribution Command (SDDC)

Construction Surveillance Technician (CST)
A citizen of the United States, who is at least 18 years of age, cleared at the TOP SECRET level, experienced in construction and trained in accordance with the Construction Surveillance Technician (CST) Field Guidebook to ensure the security integrity of a site.

Continental United States (CONUS)
United States (U.S.) territory, including adjacent territorial waters, located within the North American content between Canada and Mexico.

Contingency Plan
Plan maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Continuity of Operations (COOP)
The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to

accomplish a military action or mission in carrying out the national military strategy.

Continuous Evaluation
A formal program designed to provide information regarding an individual's continued clearance eligibility or eligibility to occupy a sensitive position.

The program evaluates an individual's post-adjudication activities by applying the same standards of loyalty, trustworthiness, and reliability used during the initial adjudication.

Continuous Operation
This condition exists when a Special Access Program Facility (SAPF) is staffed and operated 24-hours a day, 7-days a week.

Continuous Sensitive Compartmented Information Facility (SCIF) Operation
This condition exists when a Sensitive Compartmented Information Facility (SCIF) is staffed and operated 24-hours a day, 7-days a week.

Contracting Officer (CO)
A Government official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts and make determinations and findings with respect thereto or any part of such authority.

The term also includes the designated representative of the Contracting Officer (CO) acting within the limits of his or her authority.

Contractor
Any industrial, educational, commercial, or other entity that has been granted a Facility Security Clearance (FCL) by a Cognizant Security Agency (CSA).

Contractor Special Security Officer (CSSO)
An individual appointed in writing by a Cognizant Security Authority (CSA) who is responsible for all aspects of Sensitive Compartmented Information (SCI) security at a United States (U.S.) Government contractor facility.

Contractor/Command Program Manager (CPM)
A contractor-designated individual who has overall responsibility for all aspects of a program.

Contractor/Command Program Security Officer (CPSO)
An individual appointed at the contractor program facility to provide security administration and management based on guidance provided by the Program Security Officer (PSO).

Control
The authority of the agency that originates information, or its successor in function, to regulate access to the information.

Controlled Access Area (CAA)
The complete building or facility area under direct physical control that can include one or more limited exclusion areas, controlled BLACK equipment areas, or any combination thereof.

Controlled Access Program (CAP)
Director of National Intelligence (DNI)-approved programs that protect national intelligence.
These include:

- Sensitive Compartmented Information (SCI): Compartments that protect national intelligence concerning or derived from intelligence sources, methods, or analytical processes.
- Special Access Programs (SAPs): Pertaining to intelligence activities (including special activities, but excluding military, operational, strategic, and tactical programs) and intelligence sources and methods.
- Restricted Collateral Information: Other than Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs) that impose controls governing access to national intelligence or control procedures beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information, and for which funding is specifically identified.

Controlled Access Program Coordination Office (CAPCO)
The Director of National Intelligence (DNI) focal point for issues dealing with the Controlled Access Program Oversight Committee (CAPOC) and the Senior Review Group (SRG).

Controlled Access Program Coordination Office (CAPCO) Authorized Classification and Control Markings Register

The Controlled Access Program Coordination Office (CAPCO) Register identifies the official classification and control markings, and their authorized abbreviations and portion markings. It provides for the allowable vocabulary for all national intelligence markings and other non-Intelligence Community (IC) markings to control the flow of information.

The CAPCO Register provides a list of the human-readable syntax for these markings, regardless of medium (hard-copy, digital, or other).

Controlled Access Program Oversight Committee (CAPOC)

The forum supporting the Director of National Intelligence (DNI) in the management of controlled access programs.

This includes the creation and continuation of Controlled Access Programs (CAPs), including Sensitive Compartmented Information (SCI) compartments and other DNI Special Access Programs (SAPs).

It includes monitoring of these programs through performance audits and evaluations as necessary.

Controlled Area/Compound

Any area to which entry is subject to restrictions or control for security reasons.

Controlled Building
A building to which entry is subject to restrictions or control for security reasons.

Controlled Cryptographic Item
A secure telecommunications device, information handling equipment ancillary device, or associated cryptographic component that is unclassified but controlled.

Controlled Cryptographic equipment and components bear the designator "Controlled Cryptographic Item."

Controlled Information
Information and indicators deliberately conveyed or denied to foreign targets in order to evoke invalid official estimates that result in foreign official actions advantageous to United States (U.S.) interests and objectives.

Controlled Interface
A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).

Controlled Substances Act (CSA)
The Controlled Substances Act (CSA), Title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, is the legal foundation of the government's fight against the abuse of drugs and other substances.

This law is a consolidation of numerous laws regulating the manufacture and distribution of narcotics, stimulants, depressants, hallucinogens,

anabolic steroids, and chemicals used in the illicit production of controlled substances.

See: Illegal Drug Use

Controlled Unclassified Information (CUI)
A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification pursuant to Executive Order (EO) 13526, "Classified National Security Information," Reference (e), but is pertinent to the national interests of the United States (U.S) or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

NOTE: The designation Controlled Unclassified Information replaces the term Sensitive but Unclassified.

See: Classification

Cooperative Program Personnel (CPP)
Foreign government personnel assigned to a Program Office (PO) that is hosted by a Department of Defense (DoD) component in accordance with the terms of an International Cooperative Program Agreement, who report to and take direction from a DoD-appointed program manager (or program manager equivalent) for the purpose of carrying out the cooperative project or program.

Foreign government representatives described in

such agreements as liaison officers or observers are not considered CPP and are treated as Foreign Liaison Officers (FLOs).

Core Secrets
Any item, process, strategy, or element of information, in which the compromise of would result in unrecoverable failure.

Corporate Family
A corporation and its subsidiaries, divisions, and branch offices.

Corporation
A legal entity governed by a set of bylaws and owned by its stockholders.

Corroborate
To strengthen, confirm, or make certain the substance of a statement through the use of an independent, but not necessarily authoritative source.

For example, the date and place of birth recorded in an official personnel file that could be used to corroborate the date and place of birth claimed on a Standard Form (SF) 86.

See: Verify

Counterintelligence (CI)
That phase of intelligence covering all activity designed to neutralize the effectiveness of adversary intelligence collection activities.

Those activities that are concerned with identifying and counteracting the security threat posed by

hostile intelligence services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism.

Counterintelligence (CI) Assessment
A Department of Defense (DoD) component's comprehensive analysis or study of a relevant Counterintelligence (CI) topic, event, situation, issue, or development. CI assessments require exhaustive amounts of research and the production timeline can range from days to months. When conducted in support of a Research, Development, and Acquisition (RDA) program with Critical Program Information (CPI), the assessment describes the threat a foreign entity (person, representative, corporation, Government, military, commercial, etc.) represents to the CPI or system assessed. The assessment is multidisciplinary as it includes an analysis of the diverse foreign collection modalities available, the relative effectiveness of each, and capability of the foreign entity to collect information about research efforts, the technology, and/or system under development. The assessment may include the impact to the DoD if the technology is compromised and be complimentary to, integrated with, or independent of the Technology-Targeting Risk Assessment (TTRA) provided by the Defense Intelligence Community (DIC).

Countermeasure (CM)
The employment of devices and/or techniques

with the objective to impair the operational effectiveness of an adversary's activity.

Countermeasures (CMs) may include anything that effectively negates an adversary's ability to exploit vulnerabilities.

Courier
A cleared employee whose principal duty is to transmit classified material to its destination.

The classified material remains in the personal possession of the courier except for authorized overnight storage.

Co-Utilization Agreement
Two or more organizations sharing the same Special Access Program Facility (SAPF).

Cover
Protective action taken to mask or conceal an operation or activity from an adversary.

Covert Operation
An operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor.

A covert operation differs from a clandestine operation in that emphasis is placed on concealment of the identity of the sponsor, rather than on concealment of the operation.

Synonymous with the law enforcement term "Undercover Operation."

Credit Check
Information provided by credit bureaus or other

reporting services to the credit history of the subject of a Personnel Security Investigation (PSI).

See: Personnel Security Investigation (PSI)

Criminal Activity

Conduct that is or may be a violation of Federal or state criminal law, the Uniform Code of Military Justice (UCMJ), the common law, and the criminal laws of foreign countries that might embarrass or otherwise be of concern to the Department of Defense (DoD).

Selective judgment should be exercised in determining what matters are to be reported based on such factors as the nature of the criminal act, the clearance level of the individual concerned, and his or her relative position in the company.

Critical and Sensitive Information List (CSIL)

Those areas, activities, functions, or other matters that a facility or organization considers most important to keep from adversaries.

Critical Design Review (CDR)

A formal review conducted on each configuration item when design is complete.

Determines that the design satisfies requirements, establishes detailed compatibility, assesses risk, and reviews preliminary product specifications.

Critical Information (CI)

Specific facts about friendly (e.g., United States (U.S.)) intentions, capabilities, or activities vitally needed by adversaries for them to plan and

act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

Critical Infrastructure (CI)
Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States (U.S.).

These Critical Infrastructures (CIs) include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of the Government.

See: Critical Infrastructure (CI) Owner and Operator

Critical Infrastructure (CI) Owner and Operator
Those entities responsible for day-to-day operation and investment in a particular asset or system.

Critical Infrastructure Information Act (CIIA)
The Critical Infrastructure Information Act (CIIA) of 2002 (Subtitle B of Title II (Sections 211-215) of the Homeland Security Act (HSA)) consists of a group of provisions that address the circumstances under which the Department of Homeland Security (DHS) may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection (CIP) program.

Critical Infrastructure Protection (CIP) Program
A Department of Defense (DoD) management program that ensures the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.

Critical Nuclear Weapons Design Information (CNWDI)
Information classified "TOP SECRET Restricted Data (RD)" or "SECRET Restricted Data (RD)" revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device.

The sensitivity of Critical Nuclear Weapons Design Information (CNWDI) is such that it is in the national interest to assure that access is granted to the absolute minimum number of employees who require it for the accomplishment of assigned responsibilities on the strictest Need-to-Know basis.

Critical Program Information (CPI)
Information about the program, technologies, and/or systems that, if compromised, would degrade combat effectiveness or shorten the expected combat-effective life of the system.

Access to this information could allow someone to kill, counter, or clone the acquisition system before or near scheduled deployment, or force a major design change to maintain the same level of effectiveness.

Cryptoanalysis Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Crypto-Equipment
Equipment used to render plain information unintelligible and restore encrypted information to intelligible form.

Cryptography
Art or science concerning the principles, means, and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form.

Crypto-Ignition Key (CIK)
A device or electronic key used to unlock the secure mode of crypto-equipment.
See: Crypto-Equipment

Cryptologic Information System (CIS)
Any Information System (IS) which directly or indirectly supports the cryptologic effort, to include support functions such as administrative and logistics, regardless of manning, location, classification, or original funding citation. This includes strategic, tactical, and support IS; terrestrial, airborne, afloat, in-garrison, and space borne IS; IS dedicated to information handling; and information-handling portions of IS that perform other functions.

Cryptology
Science concerned with data communication and storage in secure and usually secret form. It encompasses both cryptography and cryptanalysis.

Crypto-Security
The component of communications security that results from providing and properly using technically sound cryptosystems.

Custodian
An individual who has possession of, or is otherwise charged with the responsibility for safeguarding classified information.

Customer
Any customer of a seller that is an agency or instrumentality of the United States (U.S.) Government with authority under Public Law (PL) 85-804 [50 USCS §§ 1431 et seq.] to provide for indemnification under certain circumstances for third-party claims against its contractors, including, but not limited to state and local authorities and commercial entities.

Cyber Attack
A hostile act using computer or related networks or systems intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions.

The intended effects of a cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks

on computer systems which are intended to degrade or destroy the infrastructure of Command and Control (C2) capability.

A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.

Cyber Incident (Significant)
A Level 2 or Level 1 Incident on the National Cyber Risk Alert Level (NCRAL) system.

A significant cyber incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threatening public health or safety, undermining public confidence, negatively effecting the national economy, or diminishing the security posture of the nation.

See: National Cyber Alert System (NCAS); National Cyber Risk Alert Level (NCRAL)

Cyber Infrastructure
Includes electronic information, communications systems and services, and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements.

Processing includes the creation, access, modification, and destruction of information; storage includes paper, magnetic, electronic, and all other media types; and communications include sharing and distribution of information.

For example, computer systems; control systems (e.g., Supervisory Control and Data Acquisition); and networks such as the Internet and cyber services (e.g., managed security services) are part of cyber infrastructure.

Cyber Operational Preparation of the Environment (C-OPE)

Non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-on military operations.

C-OPE includes, but is not limited to, identifying data, system and network configurations, or physical structures connected to or associated with the network or system (to include software, ports, and assigned network address ranges or other identifiers) for the purpose of determining system vulnerabilities; and actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities.

NOTE: C-OPE replaces Computer Network Exploitation (CNE) or Computer Network Attack (CNA) when used specifically as an enabling function for another military operation.

Cybersecurity Act of 2012

This act (S.2105, dated February 14, 2012) was developed to enhance the security and resiliency

of the cyber and communications infrastructure of the United States.

Cybersecurity Enhancement Act (CSEA)
The Cybersecurity Enhancement Act (CSEA) of 2002 (Section 225 of the Homeland Security Act (HSA)) requires the United States Sentencing Commission to review and amend, as necessary, all guidelines and policy statements applicable to persons convicted or certain computer crimes.

Prompted by the September 11, 2001 terrorist attacks, the primary goal of the CSEA was to ensure that elevated regard was given to sentencing of cyber terrorists based upon the grave and serious nature of cyber terrorism, and increase the severity and breadth of sentencing allowed under Federal law for cybercrimes.

Cybersecurity Information Sharing Act of 2012
This act (S.2102, dated February 13, 2012) was developed to provide the authority to monitor and defend against cyber threats, to improve the sharing of cybersecurity information, and for other purposes.

Cyber Warfare (CW)
An armed conflict conducted in whole or part by cyber means, or military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict.

Cyber Warfare (CW) includes cyber attack, cyber defense, and cyber-enabling actions.

Cybersecurity
All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures.

Cybersecurity risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability or conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.

Cyberspace
A global domain consisting of the interdependent network of information technology infrastructures; includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Common usage of the term also refers to the virtual environment of information and interactions between people.

Cyberspace Operations (CO)
The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Such operations include computer network

operations and activities to operate and defend the Global Information Grid (GIG).

Cyberspace Superiority
The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations of that force, and its related land, air, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary.

Damage
A loss of friendly effectiveness due to adversary action.

Synonymous with harm.

Damage Assessment
The analysis of the impact on national security because of the disclosure of classified information to an unauthorized person.

See: Functional Damage Assessment; Physical Damage Assessment

Damage to the National Security
Harm to the national defense or foreign relations of the United States (U.S.) from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Data
Information, regardless of its physical form or characteristics, that includes written documents, Automated Information Systems (AIS), storage media, maps, charts, paintings, drawings, films, photos, engravings, sketches, working notes, and sound, voice, magnetic, or electronic recordings.

Data Aggregation
The compilation of unclassified individual data systems and data elements resulting in the totality of the information being classified.

Data Integrity
The state that exists when computerized data is the same as that in the source documents and

has not been exposed to accidental or malicious alteration or destruction. The property that data has not been exposed to accidental or malicious alteration or destruction.

Data Mining
The analysis of data for relationships that have not previously been discovered.

DD 254 (Final)
A Contract Security Classification Specification (CSCS) that is issued by a Government Contracting Activity (GCA) or Prime Contractor to extend retention authorization to contractors who wish to retain classified information beyond the terms of the contract as authorized by the DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).

DD 254 (Original)
A Contract Security Classification Specification (CSCS) that is issued by a Government Contracting Activity (GCA) or a Prime Contractor to provide original classification guidance and security requirements on a classified contract.

Original DD 254s are issued during the solicitation phase of a contract to provide classification guidance and security requirements to prospective contractors as they formulate their bids. Once the contract is awarded, another Original DD 254 is issued to the contractor who is being awarded the contract.

DD 254 (Revised)
A Contract Security Classification Specification (CSCS) that is issued by a Government Contracting Activity (GCA) or a prime contractor to change classification guidance and security requirements on a classified contract.

Dead Bolt
A lock bolt with no spring action, usually activated by a key or turn knob and that cannot be moved by end pressure.

Deadlocking Panic HardwareA panic hardware with a deadlocking latch. The latch has a device that, when in the closed position, resists the latch from being retracted.

Debriefing
The process of informing a person his or her Need-to-Know for access is terminated.

Deception
Those measures designed to mislead the enemy/adversary by manipulation, distortion, or falsification of evidence in order to induce a reaction from that adversary which is prejudicial to the adversary's interests.

Decibel
A unit of sound measurement.

Declassification
The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized

disclosure, together with removal or cancellation of the classification designation.

Declassification Authority
The official who authorized the original classification, if that official is: 1) still serving in the same position; 2) the originator's current successor in function; 3) a supervisory official of either; or 4) delegated declassification authority in writing by the agency head or the senior agency official.

Declassification Guide
A guide providing classification and declassification instructions specifically for information that is 25 years old or older and of permanent historical value.

A Declassification Guide is also the most commonly used vehicle for obtaining Interagency Security Classification Appeals Panel (ISCAP) approval of 25-year exemptions from the automatic declassification provisions of Executive Order (EO) 13526, "Classified National Security Information," as amended.

Defense Articles
Any weapons, weapon systems, munitions, aircraft, boats, or other implements of war; any property, installations, commodities, materials, equipment, supplies, or goods used for the purposes of furnishing military assistance or making military sales; any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing, repair,

servicing, storage, construction, transportation, operation, or use of any other defense article; and any component or part of any articles listed above.

Defense Central Index of Investigations (DCII)
An automated Department of Defense (DoD) repository that identifies investigations conducted by DoD investigative agencies and personnel security determinations made by DoD adjudicative authorities.

See: Defense Central Security Index

Defense Central Security Index
An automated sub-system of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all Department of Defense (DoD) Components for military, civilian, and contractor personnel.

The Defense Central Security Index will serve as the central DoD repository of security related actions in order to assist DoD security officials in making sound clearance and access determinations and provide accurate and reliable statistical data for senior DoD officials, Congressional committees, the General Accounting Office (GAO), and other authorized Federal requesters.

See: Defense Central Index of Investigations (DCII)
Defense-in-Depth

Defense Industrial Security Clearance Office (DISCO)
The Department of Defense (DoD) approach for establishing an adequate Information Assurance (IA) posture in a shared-risk environment that allows for shared mitigation through the integration of people, technology, and operations; the layering of IA solutions within and among Information Technology (IT) assets; and, the selection of IA solutions based on their relative level of robustness. A directorate of the Defense Security Service (DSS) which serves as the Central Adjudication Facility (CAF) responsible on behalf of the Department of Defense (DoD), for determining the personnel clearance eligibility of contractor employees requiring access to classified information; maintaining personnel clearance records and furnishing information to authorized activities; processing security assurances, clearances, and visits involving the United States (U.S.) and foreign countries; and monitoring the cleared contractor's continued eligibility in the National Industrial Security Program (NISP).

Defense Information Infrastructure (DII)
The shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving Department of Defense (DoD) local and worldwide information needs.

The DII encompasses:

- Information transfer and processing resources, including information and data storage, manipulation, retrieval, and display
- Connections across DoD mission support, Command and Control (C2), and intelligence computers and users through voice, data, imagery, video, and multimedia services
- Information processing and value-added services to subscribers over the Defense Information Systems Network (DISN).

NOTE: Unique user data, information, and user applications are not considered part of the DII.

See: Defense Information Systems Network (DISN)

Defense Information Systems Network (DISN)

A sub-element of the Defense Information Infrastructure (DII), the Defense Information Systems Network (DISN) is the Department of Defense's (DoD) consolidated worldwide, enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. The DISN, transparent to users, facilitates the management of information resources and is responsive to national security and defense needs under all conditions in the most efficient manner.

The DISN is an information transfer network with value-added services for supporting national defense Command, Control, Communication, and Intelligence (C3I) decision support requirements

and Classified Military Information (CMI) functional business areas.

As an information transfer utility, the DISN provides dedicated point-to-point, switched voice and data, imagery and video teleconferencing communications services.

See: Defense Information Infrastructure (DII)

Defense Information Systems Network (DISN) Designated Approving Authority (DAA)
One of four Designated Approving Authorities (DAAs) responsible for operating the Defense Information Systems Network (DISN) at an acceptable level of risk.

The four DISN DAAs are the:

1. Director of the Defense Information Systems Agency (DISA)
2. Director of the Defense Intelligence Agency (DIA)
3. Director of the National Security Agency (NSA)
4. Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6))

See: Defense Information Systems Network (DISN); Designated Approving Authority (DAA)

Defense Office of Hearings and Appeals (DOHA)
The office responsible for making denial and

revocation decisions for Department of Defense (DoD) contractors.

Defense Personnel Exchange Program (DPEP)
A program under which military and civilian personnel of the Department of Defense (DoD), defense ministries, and/or military services of foreign governments, in accordance with the terms of an international agreement, occupy positions with, and perform functions for a host organization to promote greater understanding, standardization, and interoperability.

Defense Security Service (DSS)
The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Quantico, Virginia, with field offices throughout the United States (U.S.).

The Under Secretary of Defense for Intelligence (USD(I)) provides authority, direction, and control over DSS.

DSS provides the military services, Defense Agencies, 24 Federal agencies and approximately 13,000 cleared contractor facilities with security support services.

Defense Support of Civil Authorities
Department of Defense (DoD) support, including Federal military forces, DoD career civilian and contractor personnel, and DoD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. DoD provides Defense Support of

Civil Authorities when directed to do so by the President or Secretary of Defense (SECDEF).

Defense Support of Civil Authorities can be activated via three primary mechanisms:

1. At the direction of the President;
2. At the request of another Federal agency under the Economy Act; or
3. In response to a request from the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA) under the Stafford Act.

NOTE: The second and third mechanisms require a request for assistance and approval of the SECDEF.

Defense Technical Information Center (DTIC)
The repository for research and engineering information for the Department of Defense (DoD).

The Defense Technical Information Center (DTIC) Suite of Services is available to DoD personnel, defense contractors, Federal Government personnel and contractors, and selected academic institutions. The general public can also access unclassified, unlimited information, including many full-text downloadable documents, through the public DTIC web site.

Defense Travel Briefing
Formal advisories that alert travelers to the potential for harassment, exploitation, provocation, capture, entrapment, terrorism, or criminal activity.

These briefings include recommended courses of action to mitigate adverse security and personal consequences and suggest passive and active measures to avoid becoming a target or inadvertent victim.

Defense Treaty Inspection Readiness Program (DTIRP)
A security education and awareness program pertaining to arms control.

Defensive Counter-Cyber (DCC)
All defensive countermeasures designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace.

Defensive Counter-Cyber (DCC) missions are designed to preserve friendly network integrity, availability, and security, and protect friendly cyber capabilities from attack, intrusion, or other malicious activity by proactively seeking, intercepting, and neutralizing adversarial cyber means which present such threats.

DCC operations may include military deception via honeypots and other operations; actions to adversely affect adversary and/or intermediary systems engaged in a hostile act/imminent hostile act; and redirection, deactivation, or removal of malware engaged in a hostile act/imminent hostile act.

Defensive Travel Security Briefing
Formal advisories that alert traveling personnel of the potential for harassment, exploitation,

provocation, capture, entrapment, or criminal activity.

These briefings, based upon actual experience when available, include recommended courses of action to mitigate adverse security and personal consequences. The briefings also suggest passive and active measures that personnel should take to avoid becoming targets or inadvertent victims in hazardous areas.

See: Foreign Travel Briefing

Degauss

To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing.

To reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data.

See: Degausser; Degaussing

Degausser

An electrical device or handheld permanent magnet assembly that generates a coercive magnetic force for degaussing magnetic storage media or other magnetic material.

See: Degauss; Degaussing

Degaussing

Procedure using an approved device to reduce the magnetization of a magnetic storage media to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored

data unreadable and unintelligible.
Synonymous with demagnetizing.
See: Degauss; Degausser

Delegation of Disclosure Authority Letter (DDAL)
A letter, general or subject-specific, issued by the appropriate Designated Disclosure Authority (DDA) (normally the Navy International Program Office (IPO)) to a designated Department of Navy (DON) official defining classification levels, categories, scope, foreign countries, and limitations of information that may be authorized by the designated DON official for disclosures to a foreign recipient.

A letter required as part of the Technology Assessment/Control Plan, prepared by the cognizant DoD Component, that provides detailed guidance regarding releasability of all elements of the system or technology in question. The DDL must be approved by Under Secretary of Defense for Policy (USD(P)) before any promise or release of sensitive technology.

Under no circumstances may the contents of Delegation of Authority Letter (DDAL) be disclosed or acknowledged to foreign representatives.

Deliberate Compromise of Classified Information
Any intentional act done with the object of conveying classified information to any person not officially authorized to receive the information.

Demilitarized Zone (DMZ)
Perimeter network segment that is logically between internal and external networks. Its

purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. The DMZ is also called a "screened subnet."

Denial
The act of disowning or disavowing, specifically the refusal to grant something.
See: Deception; Denial of Service (DOS)

Denial of Service (DOS)
When an action(s) result in the inability to communicate and/or the inability of an Automated Information System (AIS) or any essential part to perform its designated mission, either by loss or degradation of a signal or operational capability.

Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)
The Department of Defense (DoD) process to ensure that risk management is applied on Information Systems (IS) through a structured process of Certification and Accreditation (C&A) to ensure and maintain the Information Assurance (IA) posture of the IS throughout the system's lifecycle.
NOTE: The DoD Information Assurance Certification and Accreditation Process

(DIACAP) replaced the predecessor DoD Information Technology Security Certification and Accreditation Process (DITSCAP) as the DoD security paradigm with the inclusion of IA controls in the C&A process.

See: Certification and Accreditation (C&A); Information Assurance (IA)

Department of Defense Components (DODC)
Identified as the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense.

Department of Defense (DoD) Directive
A Department of Defense (DoD) issuance that transmits information required by law, the President, or the Secretary of Defense that applies to all branches of DoD on the way they initiate, govern, or regulate actions. DoD Directives establish or describe policy, programs, and organizations; define missions; provide authority; and assign responsibilities. DoD Directives do not prescribe one-time tasks or deadline assignments.

Department of Defense (DoD) Instruction
A Department of Defense (DoD) issuance that implements policies and tells the user how to carry out a policy, operate a program or activity, and assign responsibilities.

Department of Defense (DoD) Publication
A DoD issuance that implements or supplements DoD Directives and DoD Instructions. DoD Publications provide standard procedures about how users shall manage or operate systems and distribute administrative information. Publications include catalogs, directories, guides, handbooks, indexes, inventories, lists, manuals, modules, pamphlets, plans, regulations, standards, and supplements.

Department of Defense Information System (DODIS)
Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Includes Automated Information System (AIS) applications, enclaves, outsourced Information Technology (IT)-based processes, and platform IT interconnections.

Department of Energy (DOE)
The Department of Energy's (DOE) overarching mission is to advance the national, economic, and energy security of the United States (U.S.), promote scientific and technological innovation in support of that mission, and ensure the environmental cleanup of the national nuclear weapons complex.

Department of Homeland Security (DHS)
In response to the terrorist attacks of September 11, 2001, the Department of Homeland Security

(DHS) was created by the Homeland Security Act (HSA) under the administration of President George W. Bush. With the primary objective to protect U.S. citizens and interests from terrorist attack, DHS is divided into five directorates: Border and Transportation Security; Emergency Preparedness and Response; Science and Technology; Information Analysis and Infrastructure Protection; and Management, with the largest directorate being Border and Transportation Security.

See: Homeland Security Act (HSA)

Department of State (DOS)

The Department of State (DOS) is the Federal executive department responsible for international relations. Among its stated missions is to advance freedom for the benefit of the American people and the international community by helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed states that respond to the needs of their people, reduce widespread poverty, and act responsibly within the international system. DOS formulates, coordinates, and provides oversight of foreign policy.

Department of the Treasury (TREAS DEPT)

The Department of the Treasury (TREAS DEPT) is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States. TREAS DEPT is responsible for a wide range of activities, such as

advising the President on economic and financial issues, encouraging sustainable economic growth, and fostering improved governance in financial institutions.

The Department operates and maintains systems that are critical to the Nation's financial infrastructure, such as producing coins and currency, disbursing payments to the public, collecting revenue, and borrowing funds necessary to run the Federal Government.

Department/Agency/Organization (DAO) Code

A 6-digit identification number assigned by the Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) Central Facility to organizational descriptions.

The Department/Agency/Organization (DAO) Code must be used by units when placing an order for STU-III/STE keying material.

See: Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE)

Derivative Classification

The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that applies to the source information.

Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Derogatory Information
Information that could adversely reflect on a person's character, trustworthiness, loyalty, or reliability, for example, a history of drug abuse or criminal activity. Information that is unrelated to character, such as foreign connections while of adjudicative significance, is not derogatory information. Generally, derogatory information is characterized as minor or significant.

See: Minor Derogatory Information; Significant Derogatory Information

Designated Approving Authority (DAA)
The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

Designated Approving Authority (DAA) Representative
An official delegated by the Designated Approving Authority (DAA) as responsible for ensuring conformance to prescribed security requirements for components of sites under purview.

Designated Courier
Individual whose temporary responsibility is to courier Sensitive Compartmented Information (SCI) material. The individual must be active-duty military, or a United States (U.S.) Government

civilian employee, contractor, or consultant meeting Director of Central Intelligence Directive (DCID) 1/14 standards specifically designated for that purpose, authorized access to the SCI material they are transporting, or holding a Proximity approval.

They must be familiar with all rules and regulations governing couriers and couriered information, and if applicable, those Federal Aviation Administration (FAA) and local policies and procedures for screening persons carrying classified material on commercial aircraft.

Designated Disclosure Authority (DDA)
An official, at subordinate component level, designated by the Head of a DoD Component or the Component's Principal Disclosure Authority to control disclosures of classified military information by his or her organization.

Designated Intelligence Disclosure Official (DIDO)
The heads of Intelligence Community (IC) organizations or those United States (U.S.) Government Officials who have been designated by the Director of National Intelligence (DNI), in writing, as having the authority to approve or deny disclosure or release of uncaveated intelligence information to foreign governments in accordance with applicable disclosure policies and procedures.

Destroying
Destroying is the process of physically damaging the media to the level that the media is not usable, and that there is no known method of retrieving the data.

Detectable Actions
Physical actions, or whatever can be heard, observed, imaged, or detected by human senses, or by active and/or passive technical sensors, including emissions that can be intercepted.

Determination Authority
A designee of a Senior Official of the Intelligence Community (SOIC) with responsibility for decisions rendered with respect to Sensitive Compartmented Information (SCI) access eligibility or ineligibility.

Deviation (Personnel Security)
Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or an out-of-date investigation.

A significant gap for this purpose is defined as either complete lack of coverage for a period of 6 months or more within the most recent 5 years investigated, the lack of a Federal Bureau of Investigation (FBI) name check or technical check, or the lack of one or more relevant investigative scope components (e.g., employment checks, financial review) in its entirety.

See: Condition (Personnel Security); Exception (Personnel Security); Waiver (Personnel Security)

Digital Signature
A cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation. An electronic signature that is a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the Signer's public key can accurately determine:

1. Whether the transformation was created using the private key that corresponds to the signer's public key; and
2. Whether the initial message has been altered since the transformation was made.

See: Public Key; Public Key Infrastructure (PKI)

Digraph
A two-letter acronym for the assigned code word or nickname.
See: Trigraph

Direction Finding
A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment.

Directive
An authoritative decision from an official body, which may or may not have binding force.

Disclosure
The release of information through approved channels.

Disclosure Record
A record of names and dates of initial access to any program information.

Discretionary Access Control (DAC)
A means of restricting access to objects (e.g., files and data entities) based on the identity and Need-to-Know status of subjects (e.g., users and processes) and/or groups to which the object belongs.

Discretionary Access Controls (DACs) are "discretionary" in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject, unless restrained by Mandatory Access Control (MAC).

See: Mandatory Access Control (MAC); Role-Based Access Control (RBAC)

Diskette
A metal or plastic disk coated with iron oxide, on which data is stored for use by an Information System (IS).

The diskette is circular and rotates inside a square lubricated that allows the read/write head access to the diskette.

Disposable Records
Federal records approved for disposal, either

immediately or after a specified retention period.
See: Temporary Records

Disposition
Indicates that a matter, item, or concept has been satisfactorily completed. It can also mean a person's character traits, dealing mainly with the person's outlook on life.

Dissemination
The provision of national intelligence to consumers in a form suitable for use.

Document
Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

Documentary Information
Any information, which is recorded on paper, film, transparency, electronic medium, or any other medium. This includes, but is not limited to printed publications, reports, correspondence, maps, audiotapes, email, spreadsheets, databases and graphical slides, technical drawings, software code, and information embodied in hardware.

Domain
An environment or context that includes a set of

system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Downgrading
A determination by a Declassification Authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Drug Enforcement Administration (DEA)
The Drug Enforcement Administration (DEA) is a United States (U.S.) Department of Justice (DOJ) law enforcement agency tasked with combating drug smuggling and use within the U.S.

The DEA is the lead agency for domestic enforcement of the drug policy of the U.S. (sharing concurrent jurisdiction with the Federal Bureau of Investigation (FBI)). It also has sole responsibility for coordinating and pursuing U.S. drug investigations abroad.

Dual Citizen
Any person who is simultaneously a citizen of more than one country.

Dual Technology
Passive infrared, microwave, or ultrasonic Intrusion Detection System (IDS) sensors which combine the features of more than one volumetric technology.

Dynamic Random-Access Memory (DRAM)
A read-write Random-Access Memory (RAM)

whose storage cells are based on transistor-capacitor combinations, in which the digital information is represented by charges that are stored on the capacitors and must be repeatedly replenished in order to retain the information.

See: Ferroelectric Random-Access Memory (FRAM); Static Random-Access Memory (SRAM)

Economic Intelligence (ECINT)
Intelligence regarding economic resources, activities, and policies.

Electrically Erasable Programmable Read-Only Memory (EEPROM)
A Read-Only Memory (ROM) using a technique similar to Erasable Programmable Read-Only Memory (EPROM), but with the capability to discharge data electrically. Usually bytes or words can be erased and reprogrammed individually during system operation.

See: Erasable Programmable Read-Only Memory (EPROM)

Electronic Attack (EA)
Division of Electronic Warfare (EW) involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA is considered a form of fires.

See: Electronic Protection (EP); Electronic Warfare (EW); Electronic Warfare Support (EWS)

Electronic Intelligence (ELINT)
Technical and geo-location intelligence derived from foreign non-communications transmissions (e.g., radar) by other than nuclear detonations or radioactive sources.

Electronic Protection (EP)
A division of Electronic Warfare (EW) involving

actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.

See: Electronic Attack (EA); Electronic Warfare (EW); Electronic Warfare Support (EWS)

Electronic Questionnaire for Investigative Processing (e-QIP)
An Office of Personnel Management (OPM) software program for the preparation and electronic submission of security forms for a Personnel Security Investigation (PSI) or suitability determination.

Electronic Security (ELSEC)
Protection resulting from measures designed to deny unauthorized persons information from the interception and analysis of non-communication electromagnetic emissions.

Electronic Surveillance (ES)
Acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of the transmitter.

Electronic Surveillance (ES) may involve consensual interception of electronic

communication and the use of tagging, tracking, and location devices.

NOTE: For the purpose of this glossary, this definition is general. A more precise statutory definition may be found in Title 50, Foreign Intelligence Surveillance Act (FISA).

Electronic Transmission (ET)
A transmission system that uses the flow of electric current (usually 4 - 20 milliamperes (ma)) to transmit output or input signals.

Electronic Warfare (EW)
Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

The three major subdivisions within Electronic Warfare (EW) are Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (EWS).

See: Electronic Attack (EA); Electronic Protection (EP); Electronic Warfare Support (EWS)

Electronic Warfare Support (EWS)
The Division of Electronic Warfare (EW) involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning

and conduct of future operations.

See: Electronic Attack (EA); Electronic Protection (EP); Electronic Warfare (EW)

Eligibility
A determination that a person meets personnel security standards for access to program material.

Emanation Security (EMSEC)
Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems.

Synonymous with Transient Electromagnetic Pulse Emanation Standard (TEMPEST).

Emergency Action Plan (EAP)
A plan developed to prevent loss of national intelligence; protect personnel, facilities, and communications; and recover operations damaged by terrorist attack, natural disaster, or similar events.

Emission Security (EMSEC)
The component of Communications Security (COMSEC) which results from all measures taken to deny unauthorized persons valuable information that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

Employee
A person, other than the President and Vice President of the United States (U.S.), employed

by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

Enclave
Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

Enclaves always assume the highest mission assurance category and security classification of the Automated Information System (AIS) applications or outsourced Information Technology-based processes they support, and derive their security needs from those systems.

Examples of enclaves include Local Area Networks (LANs) and the applications they host, backbone networks, and data processing centers.

Entrance National Agency Check (ENTNAC)
A Personnel Security Investigation (PSI) scoped and conducted in the same manner as a National Agency Check (NAC) except that a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI) is not conducted.

See: National Agency Check (NAC); Personnel Security Investigation (PSI)

Equal Employment Opportunity Commission (EEOC)
The Equal Employment Opportunity Commission (EEOC) is a Federal law enforcement agency that enforces laws against workplace discrimination. The EEOC investigates discrimination complaints based on an individual's race, color, national origin, religion, sex, age, disability, genetic information, and retaliation for reporting, participating in and/or opposing a discriminatory practice.

NOTE: The EEOC is one of the successor agencies to the Civil Service Commission (CSC).

See: Civil Service Commission (CSC)

Equipment Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone (ETZ)
A required secure distance (zone) assigned to equipment based on the Transient Electromagnetic Pulse Emanation Standard (TEMPEST) electric field radiation characteristics of equipment compared to the limits of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92.

See: Facilities Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone (FTZ)

Equity
Information originally classified by or under the control of an agency.

Erasable Programmable Read-Only Memory (EPROM)
A Read-Only Memory (ROM) in which stored data can be erased by ultraviolet light or other means and reprogrammed bit by bit with appropriate voltage pulses.

In comparison, to Electrically Erasable Programmable Read-Only Memory (EEPROM), Erasable Programmable Read-Only Memory (EPROM) devices must be saved when power is removed.

Similar products using a nitride negative-channel metal-oxide semiconductor process are termed Electrically Alterable Read-Only Memory (EAPROM).

See: Electrically Erasable Programmable Read-Only Memory (EEPROM)

Escort
A cleared person who accompanies a shipment of classified material to its destination.

The classified material does not remain in the personal possession of the escort, but the conveyance in which the material is transported remains under the constant observation and control of the escort.

Espionage
The act or practice of spying or of using spies to obtain secret intelligence.

Overt, covert, or clandestine activity, usually used in conjunction with the country against which such

an activity takes place (e.g., espionage against the United States (U.S.)).

Essential Elements of Friendly Information (EEFI)
Specific pieces of information regarding "friendly" intentions, capabilities, and activities which are likely to be sought by enemies or competitors.

Essential Elements of Information (EI)
Specific pieces of information which are likely to be sought by "friendly" planners about specific adversaries' intentions, capabilities, and activities.

Essential Secrecy
The condition achieved by denial of critical information to adversaries.

Event
An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

Exception (Personnel Security)
An adjudicative decision to grant initial or continued access eligibility despite failure to meet the full adjudicative or investigative standards. Only the head of the agency concerned or designee will make such decisions. An exception precludes reciprocity without review of the case by the gaining organization or program.

There are three types: Condition, Deviation, and Waiver.

See: Condition (Personnel Security); Deviation (Personnel Security); Waiver (Personnel Security)

Executive Order (EO)
An order issued by the President to create a policy and regulate its administration within the Executive Branch.

Exempted
Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under Executive Order (EO) 13526, "Classified National Security Information," as amended.

Expanded National Agency Check (ENAC)
Consists of investigative inquiries (record reviews and/or interviews), as necessary, to determine if investigative issues are present, or to substantiate or disprove unfavorable information disclosed during the conduct of an National Agency Check (NAC).
See: National Agency Check (NAC); Personnel Security Investigation (PSI)

Expanded Steel
A lace work patterned material produced from 9/11 gauge sheet steel by making regular uniform cuts and then pulling it apart with uniform pressure. Also called expanded metal mesh.

Exploitation
The process of obtaining and taking advantage of intelligence information from any source.

Export
The sending or taking a defense article out of

the United States (U.S.) in any manner, except by mere travel outside the U.S. by a person whose personal knowledge includes technical data; or, transferring registration or control to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List (USML), whether in the U.S. or abroad; or, disclosing (including oral or visual disclosure) or transferring in the U.S. any defense article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic mission); or, performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the U.S. or abroad.

Export License (EL)
The authorization issued by the Department of State (DOS), Office of Defense Trade Controls (ODTC), or by the Bureau of Industry and Security (BIS), Department of Commerce (DOC), which permits the export of International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EARS)-controlled articles, technical data, or services.

Export License Application (ELA)
A request submitted by United States (U.S.) persons and foreign government entities in the U.S. to export of International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EARS)-controlled articles, technical data, or services.

Extraordinary Security Measure (ESM)
A security measure necessary to adequately

protect particularly sensitive information but which imposes a substantial impediment to normal staff management and oversight.

Extraordinary security measures include:

- Program access non-disclosure agreements (read-on statements)
- Specific officials authorized to determine Need-to-Know (Access Approval Authority (AAA)
- Nicknames or code words for program identification
- Special access required markings
- Program billet structure
- Access roster
- Use of cover
- Use of special mission funds or procedures
- Use of a Special Access Program (SAP) facility or vault
- Use of a dedicated SAP Security Manager (SM)
- Any other security measure beyond those required to protect collateral information

Facilities Accreditation
An official determination of the physical, procedural and technical security acceptability of a facility that authorizes its use to protect classified national security information.

Facilities Certification
An official notification to the accreditor of the facility. Procedural and technical security acceptability of a facility to protect classified national security information.

Facility
A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operational entity.

NOTE: Entities such as military bases, industrial sites, and office complexes may be identified as facilities.

Facility Security Clearance (FCL)
An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category and all lower categories.

Facility Security Officer (FSO)
A United States (U.S.) citizen employee, who is cleared as part of the Facility Security Clearance (FCL), responsible for supervising and directing security measures necessary for implementing applicable DoD 5220.22-M, National Industrial

Security Program Operating Manual (NISPOM) and related Federal requirements for the protection of classified information.

Facility Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone (FTZ)
A space assignment based on the measured ability of the facility structure to meet the limits of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) Transient Electromagnetic Pulse Emanation Standard (TEMPEST)/1-92.

See: Equipment Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone (ETZ)

Federal Information Security Management Act (FISMA)
The Federal Information Security Management Act (FISMA) was enacted in 2002 as Title III of the E-Government Act of 2002 (Public Law (PL) 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States (U.S.).

The act requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and Information Systems (IS) that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federal Labor Relations Authority (FLRA)
The Federal Labor Relations Authority (FLRA) is an independent agency of the United States (U.S.) Government that governs labor relations between the Federal Government and its employees.

NOTE: The FLRA is one of the successor agencies to the Civil Service Commission (CSC).

See: Civil Service Commission (CSC)

Federal Personnel Manual (FPM)
Manual issued and updated by the Office of Personnel Management (OPM) and designed to administer the personnel management of civilian employees of the Federal Government.

Federal Record
Includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States (U.S.) Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

NOTE: Library and museum material made or acquired and preserved solely for reference, and stocks of publications and processed documents are not included.

Ferroelectric Random-Access Memory (FRAM)
A trademarked type of non-volatile memory developed by Ramtron International Corporation. FRAM combines the access of speed of Dynamic Random-Access Memory (DRAM) and Static Random-Access Memory (SRAM) with the non-volatility of Read-Only Memory (ROM). Because of its high speed, it is replacing Electrically Erasable Programmable Read-Only Memory (EEPROM) in many devices.

See: Dynamic Random-Access Memory (DRAM); Electrically Erasable Programmable Read-Only Memory (EEPROM); Non-Volatile Memory (NVM); Static Random-Access Memory (SRAM)

File Control Block (FCB)
A Microsoft Disk Operating System (MS-DOS) data structure that stores information about an open file. The number of FCBs is configured in CONFIG.SYS with a command "FCBS=x,y" where x (between 1 and 255 inclusive, default 4) specifies the number of file control blocks to allocate and therefore the number of files that MS-DOS can have open at one time.

See: Integral File Block

File Series
File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or

have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Financial Crimes Enforcement Network (FINCEN)
An activity of the Department of the Treasury (TREAS DEPT) that supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes.

The Financial Crimes Enforcement Network (FINCEN) provides United States (U.S.) policymakers with strategic analyses of domestic and worldwide money laundering developments, trends, and patterns.

The FINCEN works toward those ends through information collection, analysis, and sharing, as well as technological assistance and implementation of the Bank Secrecy Act (BSA) and other TREAS DEPT authorities.

See: Bank Secrecy Act (BSA), Department of the Treasury (TREAS DEPT)

Financial Disclosure
A personnel security requirement for clearance processing that requires subjects to provide information regarding their total financial situation (e.g., assets, liabilities, and indebtedness).

Firewall
A system designed to prevent unauthorized access to or from a private network.

Fixed Disk
A magnetic storage device used for high volume date storage and retrieval purposes which is not removable from the computer in which it operates.

Fixed Facility Checklist (FFC)
A standardized document used in the process of certifying a Sensitive Compartmented Information Facility (SCIF).

The Fixed Facility Checklist (FFC) documents all physical, technical, and procedural security information for the purpose of obtaining an initial or subsequent accreditation.

Such information shall include, but not be limited to: floor plans, diagrams, drawings, photographs, details of electrical, communications, and Heating, Ventilation and Air Conditioning (HVAC) systems.

Flash Memory
A special type of Electrically Erasable Programmable Read-Only Memory (EEPROM) that can be erased and reprogrammed in blocks instead of one byte at a time.

Many modern personal computers have their Basic Input-Output System (BIOS) stored on a flash memory chip so that it can easily update if necessary (Flash BIOS).

Flash memory is also popular in modems because it enables the modern manufacturer to support new protocols as they become standardized.

Flash memory is commonly used in Universal Serial Bus disk drives such as "Jump Drives."

See: Electrically Erasable Programmable Read-Only Memory (EEPROM)

FLUSH

A computer program which is part of the Computer Security Toolbox.

FLUSH is a Microsoft Disk Operating System (MS-DOS)-based program used to eliminate appended data with a file or files and appended data located in unallocated or free space on a disk or diskette.

See: BUSTER; Computer Security Toolbox

Foe

An opponent or adversary. Synonymous with enemy.

For Official Use Only (FOUO)

Designation applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA).

See: Freedom of Information Act (FOIA)

For Official Use Only (FOUO) Certified Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Technical Authority (CTTA)

An experienced, technically-qualified United States (U.S.) Government employee who has met established certification requirements in accordance with the Committee on National

Security Systems (CNSS)-approved criteria and has been appointed by a U.S Government department or agency to fulfill Certified Tempest Technical Authority (CTTA) responsibilities.

Forced Entry
Entry by an unauthorized individual(s) that leaves evidence of the act.

Foreground Information
All information and material jointly generated and funded pertaining to the cooperative program. This information is available for use by all participating governments in accordance with the terms of a Memorandum of Agreement (MOA).

See: Memorandum of Agreement (MOA)

Foreign Contact
Contact with any person or entity that is not a United States (U.S.) citizen.

Foreign Disclosure (FD)
The disclosure of Classified Military Information (CMI) or Controlled Unclassified Information (CUI) to an authorized representative of a foreign government or international organization.

NOTE: The transfer or disclosure of CMI or CUI to a foreign national who is an authorized employee of the United States (U.S.) Government or a U.S. contractor technically is not a "foreign disclosure," since the disclosure is not made to the person's Government.

Foreign Disclosure Point of Contact
Foreign Disclosure Points of Contact are Department of Navy (DON) officials who are appointed by the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), Component Commanders (CCs), Commanders of Systems Commands, and the Chief of Naval Research (CNR) for the coordination of foreign disclosure reviews and to facilitate a complete and timely response to foreign requests for classified military information or Controlled Unclassified Information (CUI) representing the consolidated organization position.

Foreign Disclosure Points of Contact do not hold disclosure authority, unless also appointed as a Designated Disclosure Authority (DDA).

Foreign Exchange Personnel
Military or civilian officials of a foreign defense establishment (Department of Defense (DoD) equivalent) who are assigned to a Department of Defense Component (DoDC) in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DoDC.

Foreign Government Information (FGI)
Information provided to the United States (U.S.) Government by a foreign government or governments, an international organization of governments, or any associated element, with the expectation that the information, the source

of the information, or both, are to be held in confidence; or, information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any associated element, requiring that the information, the arrangement, or both, are to be held in confidence; or, information received and treated as Foreign Government Information (FGI) under the terms of a predecessor order to Executive Order (EO) 13526, "Classified National Security Information."

Foreign Instrumentation Signals Intelligence (FISINT)

Intelligence information derived from electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems.

Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients.

Foreign instrumentation signals include, but are not limited to, signals from telemetry, beaconry, electronic interrogators, tracking, fusing, arming, or firing command systems, and video data links.

Foreign Intelligence (FI)

Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including Counterintelligence

(CI), except for information on international terrorist activities.

See: Foreign Intelligence Entity (FIE)

Foreign Intelligence Collection Threat
The potential of a foreign power, organization, or person to overtly or covertly collect information about United States (U.S.) acquisition program technologies, capabilities, and methods of employment that could be used to develop a similar weapon system or countermeasures to the U.S. system or related operations.

Foreign Intelligence Entity (FIE)
An organization of a foreign government that engages in intelligence activities, per Department of Defense Directive (DoDD) 5240.06, "Counterintelligence Awareness and Reporting (CIAR)."

See: Foreign Intelligence (FI)

Foreign Interest
Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States (U.S.) or its possessions and trust territories, and any person who is not a citizen or national of the U.S.

Foreign Liaison Officer (FLO)
A foreign government military member or civilian employee authorized by his or her

government and certified by a Department of Defense Component (DoDC) to act as an official representative of that government in its dealings with a DoDC in connection with programs, projects, or agreements of interest to that government.

There are three types of Foreign Liaison Officers (FLOs):

1. Security Assistance.
   A foreign government representative who is assigned to a Department of Defense (DoD)/Department of Navy (DON) Component or contractor facility in accordance with a requirement that is described in a Foreign Military Sales (FMS) Letter of Offer and Acceptance (LOA).
2. Operational.
   A foreign government representative who is assigned to a DoD/DON Component in accordance with a documented requirement to coordinate operational matters, such as combined planning or combined exercises.
3. National Representative.
   A foreign government representative who is assigned to his or her national embassy or delegation in the U.S. (e.g., an attaché) to conduct liaison activities with the DoD and DoDCs.

Foreign Military Sales (FMS)
That part of security assistance authorized by the Arms Export Control Act (AECA) and conducted using formal contracts or agreements between the United States (U.S.) Government and an authorized foreign purchaser.

These contracts, called Letters of Offer and Acceptance (LOAs) are signed by both the U.S. Government and the purchasing Government or international organization and provide for the sale of defense articles and/or defense services (to include training) from Department of Defense (DoD) stocks or through purchase under DoD -managed contracts.

Foreign National
A person who is not a citizen or national of the United States (U.S.).

Foreign Ownership, Control, or Influence (FOCI)
Whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of a company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

Foreign Person
A natural person who is not a lawful permanent resident as defined by 8 United States Code (U.S.C) 1101 (a) (20), or who is not defined as a protected

individual in accordance with 8 USC 1324b (a) (3).

The term also refers to any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the United States (U.S.), as well as international organizations, foreign governments, and/or any agency or subdivision of foreign governments (e.g., diplomatic missions).

Foreign Relations of the United StatesThe official documentary historical record of major United States (U.S.) foreign policy decisions and significant diplomatic activity.

The series, produced by the Department of State's (DOS) Office of the Historian (HO), was begun in 1861 and now comprises more than 350 individual volumes. The volumes published over the last two decades increasingly contain declassified records from all the foreign affairs agencies.

Foreign Representative

A person, regardless of citizenship, who represents a foreign interest in his or her dealings with the United States (U.S.) Government, or a person who is officially sponsored by a foreign government or international organization.

A U.S. national will be treated as a foreign person when acting as a foreign representative.

Foreign Travel Briefing

Security briefing required of cleared personnel who will be travelling abroad, either officially

or unofficially, to foreign countries, professional meetings or conferences where foreign attendance is likely; or locations where there are concerns about possible foreign intelligence exploitation.

Topics generally include:

- Potential security and safety risks
- Local Points of Contact (POCs) for assistance
- Reporting requirements and procedures
- How foreign intelligence services target and approach personnel

See: Defensive Travel Security Briefing

Foreign Visit

Any contact by a foreign representative with a Department of Navy (DON) organization or contractor facility.

Such visits are of two types, based on sponsorship:

1. Official Foreign Visit

   Contact by foreign representatives under the sponsorship of their government or an international organization with a Department of Defense Component (DoDC) or Department of Defense (DoD) contractor facility. Only official visitors may have access to classified information or Controlled Unclassified Information (CUI).

2. Unofficial Foreign Visit

   Contact by foreign nationals with a DoD/DON command or activity for

unofficial purposes, such as courtesy calls and general visits to commands or events that are open to the public, or without sponsorship of their government. Such visitors shall have access only to information that has been approved for public disclosure.

Formerly Restricted Data (FRD)
Classified information jointly determined by the Department of Energy (DOE) and its predecessors and the Department of Defense (DoD) to be related primarily to the military utilization of atomic weapons and removed by the DoE from the Restricted Data (RD) category pursuant to Section 142(d) of the Atomic Energy Act (AEA) of 1954, as amended, and safeguarded as National Security Information (NSI), subject to the restrictions on transmission to other countries and regional defense organizations that apply to RD.

Freedom of Information Act (FOIA)
A provision that any person has a right, enforceable in court, of access to Federal agency records, except to the extent that such records, or portions thereof, are protected from disclosure by one of nine exemptions.

Freight Forwarder (Transportation Agent)
Any agent or facility designated to receive, process, and transship United States (U.S) material to foreign recipients. In the context of the DoD 5220.22-M, National Industrial Security Program

Operating Manual (NISPOM), an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

Friend
In relation to national security, a country, individual, or organization with which one is allied in a struggle or cause. Synonymous with ally.

Friendly
An adjective that describes an operation or activity that is carried out by a friend (e.g., friendly fire).

Functional Damage Assessment
The estimate of the effect of force to degrade or destroy the functional or operational capability of equipment, infrastructures, and associated Information Systems (IS), and/or supporting applications to perform its intended mission and on the level of success in achieving operational objectives.

Gauss
A unit of measure of magnetic flux density.
See: Degauss

General Services Administration (GSA)
An independent agency of the United States (U.S.) Government established in 1949 to help manage and support the basic functioning of Federal agencies. The GSA supplies products and communications for U.S. Government offices, provides transportation and office space to Federal employees, and develops Government-wide cost-minimizing policies, among other management tasks.

Global Information Grid (GIG)
Defined as the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and the National Security System (NSS).

See: United States Strategic Command (USSTRATCOM)

Global Information Infrastructure (GII)
The information systems of all countries, international and multinational organizations, and

multi-international commercial communications services.

See: Defense Information Infrastructure (DII)

Government Accounting Office (GAO)
The audit, evaluation, and investigative arm of the United States (U.S.) Congress and Legislative Branch.

The stated mission of the GAO is: "The agency exists to support the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the Federal Government for the benefit of the American people."

Government Contracting Activity (GCA)
An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Government Program Manager (GPM)
The Senior Government program official who has ultimate responsibility for all aspects of the program.

Government-Approved Facility
Any Government-owned room or outside of a Special Access Program Facility (SAPF) with controlled or restricted access designed to limit public access which has operational procedures in place to actually limit access; any Government-owned SAPF or area within a SAPF.

Government-Off-The-Shelf (GOTS)
An item that has been developed by the Government and produced to military or commercial standards and specifications, is readily available for delivery from an industrial source, and may be procured without change to satisfy a military requirement.
See: Commercial Off-The-Shelf (COTS)

Government-to-Government Channels
The principle that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed upon by the governments involved. In either case, the information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.

Government-to-Government Transfer (G2G)
The principle that classified information and material will be transferred by Government officials through official Government channels (e.g., military postal service, diplomatic courier) or through other channels expressly agreed upon in writing by the Governments involved.

In either case, the information or material may be transferred only to a person specifically designated in writing by the foreign government as its designated Government representative for that purpose.

Granularity
Relative fineness to which an access control mechanism can be adjusted.

Guard
A properly trained and equipped individual whose duties include the protection of a Special Access Program Facility (SAPF).

Guards will be United States (U.S.) citizens and their primary duty will focus on the protection of U.S. Government classified information. Guards will possess a U.S. SECRET clearance.

Guest System
Any system that enters the Special Access Program Facility (SAPF) which has not already been certified or accredited by the respective cognizant SAPF authority is considered a guest system.

Hacker
An individual who gains unauthorized access to an Automated Information System (AIS).

Hand Carrier
A cleared employee who occasionally hand carries classified material to its destination in connection with a classified visit or meeting.

The classified material remains in the personal possession of the hand carrier except for authorized overnight storage.

Handle Via Special Access Control Channels Only
A protective marking used within Special Access Program (SAP) control channels. It is used to identify unclassified information which requires protection in Special Access channels.

When Handle Via Special Access Channels Only is used to help identify classified SAP information, the material will be protected in accordance with the security requirements of the individual SAP or the highest standard where more than one SAP is included.

See: For Official Use Only (FOUO)

Hard Disk
A magnetic storage device used for high volume data storage and retrieval purposes, to include ones which are both removable and non-removable from the computers in which they operate.

Hardcopy Document
Any document that is initially published and distributed by the originating component in paper form and that is not stored or transmitted by electrical means.

Hardened Cable Path
A material, container, or facility that provides physical protection for the cable and causes a delay to a perpetrator attempting unauthorized penetration or intrusion.

Head of Department of Defense Component
The Secretary of Defense (SECDEF); the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff (CJCS); the Commanders of Unified and Specified Commands; and the Directors of Defense Agencies.

Home Office Facility
The headquarters facility of a multi-facility organization.

Homeland Security Act (HSA)
The Homeland Security Act (HSA) (PL 107-296) was enacted under the under the administration of President George W. Bush on November 25, 2002 in response to the September 11, 2001 terrorist attacks.

The HSA provided broad powers to Federal law enforcement agencies to protect citizens and interests from terrorist attacks within the United States (U.S.).

The legislation provided for the establishment of the U.S. Department of Homeland Security

(DHS) and cabinet-level position of Secretary of Homeland Security. Included in the legislation are the Critical Infrastructure Information Act (CIIA) (Subtitle B of Title II (Sections 211-215)) and the Cyber Security Enhancement Act (CSEA) (Section 225).

See: Department of Homeland Security (DHS); Critical Infrastructure Information Act (CIIA); Cyber Security Enhancement Act (CSEA)

Hostile Act
Force or other means used directly to attack the United States (U.S.), U.S. forces, or other designated persons or property, to include critical cyber assets, systems, or functions. The term also includes force or other means to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital U.S. Government property.

Hostile Intent
The threat of an imminent hostile act.

Human Intelligence (HUMINT)
A category of intelligence derived from information collected and/or provided by human sources.

Illegal Drug Use
The use, possession, or distribution of drugs, which is unlawful under the Controlled Substances Act (CSA).

Such term does not include the use of a drug taken under the supervision of a licensed health care professional, other uses authorized by the CSA, or other provisions of law.

See: Controlled Substances Act (CSA)

Imagery
Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

Imagery Intelligence (IMINT)
Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar, wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media.

Imitative Communications Deception
Introduction of deceptive messages or signals into an adversary's telecommunications signals.

Immediate Family Member
Mother, father, sister, brother, spouse, son, daughter.

Each of these terms includes all its variants (e.g., "sister" includes sister by blood, sister by adoption, half-sister, stepsister, and foster sister).

NOTE: For purposes of determining access eligibility, cohabitants have a status identical to that of immediate family.

Immigrant Alien
Any alien lawfully admitted into the United States (U.S.) under an immigration visa for permanent residence.

Immigration Reform and Control Act (IRCA)
The Immigration Reform and Control Act (IRCA) was enacted in 1986 to control and deter illegal immigration to the United States (U.S.).

The major provisions of IRCA stipulate legalization of undocumented aliens who had been continuously unlawfully present since 1982, legalization of certain agricultural workers, sanctions for employers who knowingly hire undocumented workers, and increased enforcement at U.S. borders.

Inadvertent Disclosure
A set of circumstances or a security incident in which a person has had involuntary access to classified information that he or she was or is not normally authorized.

Incident
An assessed event of attempted entry, unauthorized entry, and/or attack against a facility, operation, or Automated Information System (AIS).

Incident of Security Concern
Events that, at the time of occurrence, cannot be determined to be an actual violation of law, but which are of such significance as to warrant preliminary inquiry and subsequent reporting. Examples include drug use and distribution, alcohol abuse, the discovery or possession of contraband articles in security areas, and unauthorized attempts to access classified data.

Independent Research and Development (IR&D)
A contractor-funded research and development effort that is not sponsored by, or required in performance of, a contract or grant that consists of projects falling within the areas of basic research, applied research, development, systems, and/or other concept formulation studies.

Indoctrination
An initial indoctrination and/or instruction provided to each individual approved to a Special Access Program (SAP) prior to exposure concerning the unique nature of program information and the policies, procedures, and practices for its handling.

Industrial Espionage
The act of seeking a competitive, commercial advantage by obtaining a competitor's trade secrets and/or logistics.

The acquisition of industrial information through clandestine operations.

Industrial Security
The portion of information security that is concerned with the protection of classified information in the custody of United States (U.S.) industry.

Information
Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by, or for, or is under the control of the United States (U.S.) Government.

"Control" refers to the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information and Communications Technology
An umbrella term that includes information technology (IT) and any communication devices or applications, encompassing radio, television, cellular phones, computer and network hardware and software, satellite systems, etc., as well as the various services and applications associated with them, such as videoconferencing and distance learning.

Information Assurance (IA)
Information operations that protect and defend information and Information Systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance (IA) Control
An objective condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (e.g., a control number, a control name, control text, and a control class).

Specific management, personnel, operational, and technical controls are applied to each Department of Defense (DoD) Information System (IS) to achieve an appropriate level of integrity, availability, and confidentiality.

See: Certification and Accreditation (C&A); Information Assurance (IA)

Information Assurance (IA) -Enabled Information Technology (IT) Product
Product or technology whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities.

Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Information Assurance (IA) Product
Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious

penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

See: Certification and Accreditation (C&A); Information Assurance (IA)

Information Assurance Manager (IAM)
The manager responsible for an organization's Information System (IS) security program. The Information Assurance Manager (IAM) is appointed by the Commander/Commanding Officer (CO), or by company management in the case of a contractor. The IAM is the single point of contact for his or her organization concerning security matters to the Designated Approving Authority (DAA).

NOTE: The title of "Information Assurance Manager (IAM)" replaced "Information Systems Security Manager (ISSM)."

Information Assurance Officer (IAO)
The individual responsible to the Information Assurance Manager (IAM) for ensuring that Operations Security (OPSEC) is maintained for a specific Information System (IS). The Information Assurance Officer (IAO) may have the responsibility for more than one system.

NOTES: The IAO may be referred to as a Network Security Officer (NSO), or a Terminal Area or Information System Security Custodian.

The title of "Information Assurance Officer (IAO)" replaced "Information Systems Security Officer (ISSO)."

Information Integrity
The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Information Operation
Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.

Information Owner
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security
The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that executive order or statute protects.

Information Security Oversight Office (ISOO)
The Information Security Oversight Office (ISOO) is responsible to the President of the United States (U.S.) for policy and oversight of the Government-wide security classification system and the National Industrial Security Program (NISP).

ISSO authority is derived from Executive

Order (EO) 13526 "Classified National Security Information" and EO 12829 "National Industrial Security Program," as amended. The ISOO is a component of the National Archives and Records Administration (NARA) and receives policy and program guidance from the National Security Council (NSC).

Information Storage Device (ISD)
The physical storage device used by an Information System (IS) upon which data is recorded.

Information System (IS)
An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Information System Security Engineer (ISSE)
The individual responsible for the engineering process that captures and refines information protection requirements and ensures their integration into Information Technology (IT) acquisition processes through purposeful security design or configuration.

Information Systems Security (INFOSEC)
Information Systems Security (INFOSEC) is the protection afforded to Information Systems (IS) in order to preserve the availability, integrity,

and confidentiality of the systems and the information contained with the system. INFOSEC encompasses the protection of information systems against unauthorized access to, or modification of, information whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. Such protection is the integrated application of Communications Security (COMSEC), Transient Electromagnetic Pulse Emanation Standard (TEMPEST), and Information Assurance (IA) executed in unison with personnel security, operations security, industrial security, resources protection, and physical security.

Information Systems Security Representative (ISSR)
The provider-assigned individual responsibility for the onsite security of the Automated Information System (AIS) processing information for the customer.

Information Warfare (INFOWAR)
Actions taken to achieve information superiority by adversely affecting an adversary's information, information-based processes, and/or information systems while defending one's own information, information-based processes, and/or information systems. Information operations conducted during time of crisis or conflict to achieve or promote

specific objectives over a specific adversary or adversaries.

Infraction
Any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a violation.

Initial Operating Capability (IOC)
A time when the organizational authoritative entity declares that a system sufficiently meets requirements for formal operational status while the system may not meet all of the original design specifications to be declared fully operational.

Insider

Anyone who has authorized access to Department of Defense (DoD) resources by virtue of employment, volunteer activities, or contractual relationship with DoD.

Insider Threat
Any circumstance or event with the potential to adversely impact agency operations, including mission, functions, image, or reputation, agency assets, or individuals through an Information System (IS) via internal unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DOS).

See: Internal Vulnerability

Inspectable Space (IS)
A determination of the three-dimensional space

surrounding equipment that processes classified and/or sensitive information within which Transient Electromagnetic Pulse Emanation Standard (TEMPEST) exploitation is not considered practical, or where legal authority to identify and remove a potential TEMPEST exploitation exists.

Integral File Block
A distinct component of a file series that should be maintained as a separate unit in order to ensure the integrity of the records.

An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

See: File Control Block (FCB)

Integrity
Quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

NOTE: In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Intelligence
The product from the collection, evaluation,

analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations and that is immediately or potentially significant to military planning and operations.

Intelligence Activity (IA)
An activity that an agency within the Intelligence Community (IC) is authorized to conduct under Executive Order (EO) 12333, "United States Intelligence Activities."

Intelligence Collection (INTCOL)
The act of gathering information from all available sources to meet an intelligence requirement.

Intelligence Community (IC)
The Intelligence Community (IC) is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. Their primary mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties. The 17 IC member agencies are:

- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency (CIA)
- Coast Guard Intelligence

- Defense Intelligence Agency (DIA)
- Department of Energy (DOE)
- Department of Homeland Security
- Department of State (DOS)
- Department of the Treasury (TREAS DEPT)
- Drug Enforcement Administration (DEA)
- Federal Bureau of Investigation (FBI)
- Marine Corps Intelligence
- National Geospatial-Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)
- Navy Intelligence
- Office of the Director of National Intelligence (ODNI)

Members of the IC collect and assess information regarding international terrorist and narcotic activities; other hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed against the United States (U.S.) As needed, the President may also direct the IC to carry out special activities in order to protect U.S. security interests against foreign threats.

Intelligence Cycle
The steps by which raw information is converted into intelligence and made available to users. The cycle has been described as including five steps: planning and direction, collection, processing, production, and dissemination.

Intelligence Information
Unevaluated material that may be used in the production of intelligence.

Intelligence Sources and Methods
Sources: Persons, images, signals, documents, databases, and communications media capable of providing intelligence information through collection and analysis programs (e.g., Human Intelligence (HUMINT), Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Geospatial Intelligence (GEOINT), and Measurement and Signature Intelligence (MASINT)).

Methods: Information collection and analysis strategies, tactics, operations, and technologies employed to produce intelligence products. If intelligence sources or methods are disclosed without authorization, their effectiveness may be substantially negated or impaired.

NOTE: The term "intelligence sources and methods" is used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence (DNI).

Intelligence Special Access Program
A Special Access Program (SAP) established primarily to protect the planning and execution of especially sensitive intelligence or Counterintelligence (CI) operations or collection activities.

Intelligence System
Any system (formal or informal) which is used to manage data by gathering, obtaining, processing,

interpreting, and providing analytically-sound opinions to decision makers so that they may make informed decisions with regard to various courses of action.

The term is not limited to intelligence organizations or services, but includes any system, in all its parts, that accomplishes the listed tasks.

Intending Citizen
An alien who falls into one of four categories under the Immigration Reform and Control Act (IRCA) of 1986.

See: Immigration Reform and Control Act (IRCA)

Intention
An aim or design to execute a specified course of action.

Intercept
Data which is obtained through the passive collection of signals, or, interrupting access, communication, or the flow of a process.

Interconnected Network
A Network Information System (NIS) comprised of two or more separately accredited systems and/or networks.

Interim Access Authorization (IAA)
A determination to grant access authorization prior to the receipt and adjudication of the individual's complicated background investigation.

See: Temporary Access Eligibility; Interim Security Clearance

Interim Approval to Operate (IAO)
Temporary authorization granted by a Designated Approving Authority (DAA) for an Information System (IS) to process classified information in its operational environment based on preliminary results of a security evaluation of the system.

Interim Security Clearance
A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

Internal Vulnerability
A weakness in an Information System (IS), system security procedures, internal controls, or implementation that could be exploited or triggered by an organic threat source.
See: Insider Threat

International Organization
An entity established by recognized governments under an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

Interoperability
The capability of one system to communicate

with another system through common protocols.

Intrusion
Unauthorized act of bypassing the security mechanisms of a system.
See: Intrusion Detection System (IDS)

Intrusion Detection System (IDS)
A security alarm system to detect unauthorized entry.

Invalidation
An administrative action that renders a contractor ineligible to receive additional classified information, except that information necessary for completion of essential contracts, as determined by the appropriate Government Contracting Agencies (GCAs).

Isolator
A device or assembly of devices which isolates or disconnects a telephone or Computerized Telephone System (CTS) from all wires which exit the Special Access Program Facility (SAPF) and has been accepted as effective for security purposes by the Telephone Security Group (TSG).
See: Computerized Telephone System (CTS); Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE)

Issue Case
A case containing any issue information, even if fully mitigated.
See: Issue Information (Personnel Security)

Joint Personnel Adjudication System (JPAS)
The centralized Department of Defense (DoD) database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities (CAFs) by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations (e.g., Defense Security Service (DSS), Defense Manpower Data Center (DMDC), Defense Civilian Personnel Management (DCPM), and the Air Force Personnel Center (AFPC)).

Joint Use Agreement (JUA)
A written agreement signed by two or more accrediting authorities whose responsibility includes information processed on a common Automated Information System (AIS) or network. Such an agreement defines a Cognizant Security Authority (CSA) and the security arrangements that will govern the operation of the network.

Joint Venture
A combination of two or more contractors without any actual partnership or corporation designation who perform or act jointly in a specific endeavor such as the negotiation for or performance of a contract.

Key Material Identification Number (KMID)
A unique number automatically assigned to each piece of Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) keying material.
See: Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE)

Key Resources
Any publicly or privately controlled resources essential to the minimal operations of the economy and Government.

Key Service Unit (KSU)
An electromechanical switching device which controls the routing and operation of an analog telephone system.

Law Enforcement Sensitive
Law Enforcement Sensitive information is defined as unclassified information of a sensitive and proprietary nature that, if disclosed, could cause harm to law enforcement activities by jeopardizing investigations, compromising operations, or causing life-threatening situations for confidential informants, witnesses, or law enforcement personnel.

Lawful Permanent Resident
Any person not a citizen of the United States (U.S.) who is residing in the U.S. under a legally recognized and lawfully recorded permanent residence as an immigrant. Also known as a "Permanent Resident Alien," "Resident Alien Permit Holder," and "Green Card Holder."

Lead
Single investigative element of a case requiring action. Leads include reference interviews, record checks, subject interviews, Local Agency Checks (LACs), and National Agency Checks (NACs).
See: Local Agency Check (LAC); National Agency Check (NAC); Personnel Security Investigation (PSI)

Letter of Compelling Need
A letter, signed by the Facility Security Officer (FSO) and Program Manager (PM), used to justify or offset the risk related to accessing an individual who does not fully meet access criteria. It describes the benefit to the specific Special Access Program (SAP) by describing the

candidate's unique talent, particular expertise, or critically-needed skill.

Letter of Intent
A letter from a Central Adjudication Facility (CAF) to a subject, notifying of the CAF's intent to deny/revoke security clearance/eligibility, and the reasons for the proposed action.

See: Unfavorable Personnel Security Determination

Level of Concern
The Level of Concern is a rating assigned to an Information System (IS) by the Designated Approving Authority (DAA). A separate Level of Concern is assigned to each IS for Confidentiality, Integrity and Availability, with further categorization as Basic, Medium, or High:

- Confidentiality: Based on the information it maintains, processes, and transmits.
- Integrity: Based on the degree for resistance to unauthorized modifications.
- Availability: Timely, reliable access to data and information services for authorized users

Limited Access Authorization (LAA)
Authorization for access to CONFIDENTIAL or SECRET information granted to non-United States (U.S.) citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years.

Limited Background Investigation (LBI)
A Limited Background Investigation (LBI) consists of a Personal Subject Interview; National Agency Check (NAC) plus credit search; personal interviews with employers (3 years), residence and educational sources (3 years); and law enforcement searches (5 years).
See: Background Investigation (BI)

Limited Liability Company (LLC)
A type of company, authorized only in certain states, whose owners and managers receive the limited liability and (usually) tax benefits of a corporation without having to conform to the corporation restrictions. An LLC is an unincorporated association, is relatively flexible, and allows for pass-through income taxation.

Line Supervision

- Class I:

  Class I line security is achieved through the use of Data Encryption Standard or an algorithm based on the Cipher feedback or Cipher block chaining mode of encryption. Certification by National Institute of Science and Technology (NIST) or another independent testing laboratory is required.
- Class II:

  Class II line supervision refers to systems in which the transmission is based on pseudo, random-generated, or digital

encoding using an interrogation and response scheme throughout the entire communication, or Underwriter's Laboratory Class AA line supervision. The signal shall not repeat itself within a minimum 6 month period and Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

Local Agency Check (LAC)
An investigative check of local police departments, courts, etc., to determine whether the subject has been involved in criminal conduct.

The Local Agency Check (LAC) is a part of all Personnel Security Investigations (PSIs) except the Entrance National Agency Check (ENTNAC).

See: Personnel Security Investigation (PSI)

Local Area Network (LAN)
A Local Area Network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area.

See: Network, Wide Area Network (WAN)

Logic Bomb
A logic bomb is a program or code fragment which triggers an unauthorized, malicious act when some predefined condition occurs. The most common type is the "time bomb", which

is programmed to trigger an unauthorized or damaging act long after the bomb is "set."

For example, a logic bomb may check the system date each day until it encounters the specified trigger date and then executes code that carries out its hidden mission. Due to the built-in delay, a logic bomb virus is particularly dangerous because it can infect numerous generations of backup copies of data and software before its existence is discovered.

See: Malicious Code

Long-Haul Telecommunications
All general purpose and special purpose long-distance facilities and services (including terminal equipment and local circuitry supporting the long-haul service) used to support the electromagnetic and/or optical dissemination, transmission, or reception of information via voice, data, video, integrated telecommunications, wire, or radio to or from the post, camp, base, or station switch and/or main distribution frame (except for trunk lines to the first-serving commercial central office for local communications services).

Low Probability of Detection (LPD)
The result of measures used to hide or disguise intentional electromagnetic transmissions.

Low Probability of Intercept (LPI)
Result of measures to prevent the intercept of intentional electromagnetic transmissions.

Malicious Code
Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an Information System (IS). The malicious code may be included in hardware, software, firmware or data. Computer viruses, worms, trojan horses, trapdoors, and logic bombs all fall under the definition of malicious code. Computer viruses pose the primary threat to an IS because of their reproductive capability.

Malicious Code Screening
The process of monitoring Information Systems (IS) for the presence of malicious code.
See: Malicious Code

Mandatory Access Control (MAC)
A system of access control that assigns security labels or classifications to system resources and allows access only to entities (people, processes, devices) with distinct levels of authorization or clearance. These controls are enforced by the operating system or security kernel.
See: Discretionary Access Control (DAC); Role-Based Access Control (RBAC)

Mandatory Declassification Review
The review for declassification of classified information in response to a request for declassification that meets the requirements under Sections 3.5 and 3.6 of Executive Order (EO) 13526, "Classified National Security Information."

Manipulative Communications Deception
Alteration or simulation of friendly telecommunications for the purpose of deception.

Master Crypto-Ignition Key Custodian
An individual at each node in a Community of Interest (COI) who is responsible for controlling and maintaining the Master Crypto-Ignition Key and programming the security features of the Secure Terminal Equipment.

See: Community of Interest (COI)

Material
Any product or substance on or in which information is embodied.

Measurement and Signature Intelligence (MASINT)
Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic). This data is derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender. This facilitates subsequent identification and or measurement of the same.

Memorandum of Agreement (MOA)
A written agreement among relevant parties that specifies roles, responsibilities, terms, and conditions for each party to reach a common goal.

Memory Component
Considered to be the Lowest Replaceable Unit (LRU) in a hardware device.

Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

Merit Systems Protection Board (MSPB)
The Merit Systems Protection Board (MSPB) serves to protect Federal merit systems against partisan political and other prohibited personnel practices and to ensure adequate protection for Federal employees against abuses by agency management.

NOTE: The MSPB is one of the successor agencies to the Civil Service Commission (CSC)

See: Civil Service Commission (CSC)

Minimum Background Investigation (MBI)
This investigation includes a National Agency Check Plus Written Inquiries (NACI), a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers.

A Minimum Background Investigation (MBI) is typically reserved for public trust positions and/or when there is a break in Federal service.

See: Background Investigation (BI)

Minor Derogatory Information
Information that, by itself, is not of sufficient

importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

Minor Issue Information
Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," but for which adjudication determines that adequate mitigation, as provided by the existing guidelines exist.

NOTE: Minor issue information does not provide the basis for waiver or condition.

See: Issue Information (Personnel Security); Substantial Issue Information

Mission Assurance Category
Applicable to Department of Defense (DoD) Information Systems (IS), the Mission Assurance Category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission.

Mission Assurance Categories are primarily used to determine the requirements for availability and integrity. DoD has three defined mission assurance categories:

- Mission Assurance Category I: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

The consequences of loss of integrity or availability of a Mission Assurance Category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

- Mission Assurance Category II: Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure adequate assurance.
- Mission Assurance Category III: Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or

degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

Mission Essential
In the context of information, that information which is an essential portion of a unit's mandatory wartime capability.

Mitigation
Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems.

Mobile Code
Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

Modulator-Demodulator (MODEM)
A device for transmitting usually digital data over telephone wires by modulating the data into an audio signal to send it and demodulating an audio signal into data to receive it (abbreviation

of Modulator-Demodulator).

Motion Detection Sensor
An alarm sensor that detects movement.

Multilevel Security
The concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

Multiple Facility Organization
A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more contactors.

Multiple Sources
Two or more source documents, classification guides, or a combination of both.

National (of the United States)
A citizen of the United States (U.S.) or a person who, though not a citizen of the U.S., owes permanent allegiance to the U.S.

National Agency Check (NAC)
A Personnel Security Investigation (PSI) consisting of a records review of certain national agencies, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

National Agency Check Plus Written Inquiries (NACI)
A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a National Agency Check (NAC), credit bureau check, and written inquires to current and former employers, covering a 5-year scope.
See: Credit Check; National Agency Check (NAC); Personnel Security Investigation (PSI)

National Agency Check with Local Agency Checks and Credit Check (NACLC)
A Personnel Security Investigation (PSI) covering the past 5-7 years and consisting of a National Agency Check (NAC), financial review, verification of date and place of birth, and Local Agency Checks (LACs).
See: Local Agency Check (LAC); National Agency Check (NAC)

National Cyber Alert System (NCAS)
The coordinated, web-based national cyber

security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats.

Managed by the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT), in partnership with the DHS National Cyber Security Division (NCSD) and the private sector, the National Cyber Alert System (NCAS) provides an infrastructure for relaying graded computer security update and warning information to all users via email.

See: Department of Homeland Security (DHS); United States Computer Emergency Readiness Team (US-CERT); National Cyber Security Division (NCSD)

National Cyber Risk Alert Level (NCRAL)

The National Cyber Risk Alert Level (NCRAL) system is designed to inform preparedness, decision making, information sharing, and cyber incident management activities.

The Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) determines the alert level in coordination with recommendations from the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and partners.

The levels include:

Level 1 (Severe): Highly disruptive levels of consequences are occurring or imminent.

Level 2 (Substantial): Observed or imminent degradation of critical functions with a

moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending.

Level 3 (Elevated): Early indications of, or the potential for, but no indicators of moderate to severe levels of consequences.

Level 4 (Guarded): Baseline of risk acceptance.

- National Cyber Security Division (NCSD) The National Cyber Security Division (NCSD) works collaboratively with public, private, and international entities to secure cyberspace, cyber assets, and the current United States (U.S.) cyber infrastructure through the following objectives:
- To build and maintain an effective national cyberspace response system
- To implement a cyber-risk management program for protection of critical infrastructure

National Information Assurance Partnership (NIAP)

Joint initiative between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) responsible for security testing needs of both Information Technology (IT) consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

National Information Infrastructure (NII)
The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users.

The National Information Infrastructure (NII) includes both public and private networks, the Internet, the public switched network, and cable, wireless, and satellite communications.

National Intelligence
All intelligence, regardless of the source from which it is derived, including information gathered within or outside the United States (U.S.) that: (a) pertains, as determined consistent with any guidance issued by the President, to more than one U.S. Government agency; and (b) involves: (i) threats to the U.S., its people, property, or interest; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on U.S. national and/or homeland security.

National Military Strategy for Cyberspace Operations (NMS-CO)
The comprehensive strategy of the United States (U.S) Armed Forces to ensure U.S. military superiority in cyberspace.

The National Military Strategy for Cyberspace Operations (NMS-CO) establishes a common understanding of cyberspace and sets forth a military strategic framework that orients and focuses Department of Defense (DoD) actions in

the areas of military, intelligence, and business operations in and through cyberspace.

National Security Agency/Central Security Service (NSA/CSS)
The National Security Agency/Central Security Service (NSA/CSS) is the Government's lead for cryptologic work in Signals Intelligence (SIGINT)/ Computer Network Exploitation (CNE), Information Assurance (IA), and network threat operations.

The primary operational functions of NSA/CSS include creating and maintaining time-sensitive capabilities to determine and disseminate the configuration and activities of networks of interest; characterizing and reporting cyber foreign threats to networks of interest in accordance with the mission to predict, detect, defeat, and attribute exploitations and attacks; conducting detection 24 hours a day, 7 days a week, alert, and incident response services to defend Department of Defense (DoD) unclassified networks; providing technical assistance, upon request and as appropriate, to Federal entities; and supporting collaborative planning and computer network operations (by NSA/CSS, United States Strategic Command (USSTRATCOM), and the broader community of the United States (U.S.), its allies, and its mission partners).

National Security and Emergency Preparedness (NS/EP) Communications
Those communications services which are used to maintain a state of readiness or to respond to

and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the National Security and Emergency Preparedness (NS/EP) posture of the United States (U.S.).

National Security Information (NSI)
Information that has been determined, pursuant to Executive Order (EO) 13526, "Classified National Security Information," or any predecessor order, to require protection against unauthorized disclosure.

National Security-Related Information
Unclassified information related to national defense or foreign relations of the United States (U.S.).

Naval Nuclear Propulsion Information (NNPI) Information
Classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities. Information concerning equipment, components, or technology which is applicable to both naval nuclear and conventional propulsion plants is not considered to be Naval Nuclear Propulsion Information (NNPI) when used in reference to conventional applications only, provided no association with naval nuclear propulsion can be directly identified from the information in question.

Need for Access
A determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized Governmental function.

Need-to-Know
A determination which is made by an authorized holder of classified or proprietary information as to whether or not a prospective recipient requires access to the specific information in order to perform or assist in a lawful and authorized Governmental function.

Need-to-Know Determination
Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (DoD Directive 8500.1).

Network
A computing environment with more than one independent processor interconnected to permit communications and sharing of resources.

See: Local Area Network (LAN); Wide Area Network (WAN)

Network Manager (NETMGR)
The individual who has supervisory or management responsibility for an organization, activity, or functional area that owns or operates a network.

Network Operations (NetOps) Activities
Conducted to operate and defend the

Department of Defense (DoD) Global Information Grid (GIG).

Network Security Officer
An individual formally appointed by a Designated Approving Authority (DAA) to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an Information Systems (IS) network.

See: Information Assurance Officer (IAO)

Network System
A system that is implemented with a collection of interconnected network components. A network system is based on a coherent security architecture and design.

See: Network

Newly Discovered Records
Records that were inadvertently not reviewed prior to the effective date of automatic declassification because the Agency's Declassification Authority was unaware of their existence.

Nicknames
A combination of two separate unclassified words assigned to represent a specific Special Access Program (SAP) or portion thereof.

Non-Conductive Section
Material, such as canvas or rubber, installed in ducts, vents, or pipes, that is unable to carry audio or radio frequency emanations.

Non-Disclosure Agreement (NDA)
An official authorized contract between an individual and the United States (U.S.) Government signed by an individual as a condition of access to classified national intelligence. The NDA specifies the security requirements for access and details the penalties for non-compliance.

Non-Discussion Area
A clearly defined area within a Special Access Program Facility (SAPF) where classified discussions are not authorized due to inadequate sound attenuation.

See: Sound Attenuation

Non-Record Material
Certain documentary materials that are specifically excluded by law (44 United Stated Code (U.S.C.) 3301) from the records of the Federal Government, based upon the following: 1) the nature of the material; 2) the relationship to records; and 3) the use of the material.

Non-Repudiation
Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data. Digital signatures are the current non-repudiation technique of choice for the National Information Infrastructure (NII).

See: National Information Infrastructure (NII)

Non-Secure Internet Protocol Router Network (NIPRNET)
Used to exchange sensitive but unclassified information between "internal" users as well as provide users access to the Internet. The NIPRNET is composed of Internet Protocol (IP) routers owned by the Department of Defense (DoD). It was created by the Defense Information Systems Agency (DISA) to supersede the earlier Military Network.
See: Unclassified Internet Protocol Router Network

Non-Volatile Memory (NVM)
Computer memory that retains data even when all power sources are disconnected. Examples include Read-Only Memory (ROM), Flash Memory, Ferroelectric Random-Access Memory (FRAM), most types of magnetic computer storage devices (e.g., hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.
See: Volatile Memory; Non-Volatile Random-Access Memory (NVRAM)

Non-Volatile Random-Access Memory (NVRAM)
Random-Access Memory (RAM) that retains its information when power is turned off (non-volatile). This is in contrast to volatile Dynamic Random-Access Memory (DRAM) and Static Random-Access Memory (SRAM), which both maintain data only for as long as power is applied.
See: Dynamic Random-Access Memory (DRAM);

Volatile Memory (VM); Static Random-Access Memory (SRAM)

North Atlantic Treaty Organization (NATO) Classified Information
All classified information—military, political, and economic—circulated within North Atlantic Treaty Organization (NATO), whether such information originated in NATO or is received from member nations or from international organizations.

Object Reuse
The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects.

To be securely reassigned, such media will contain no residual data from the previously contained object(s).

Observables
Any actions that reveal indicators which are exploitable by adversaries.

Oersted (Oe)
The unit of measure of a magnetic field.

See: Coercive Force; Coercivity

Offensive Cyberspace Operations (OCO)
Offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible.

The goal of Offensive Cyberspace Operations (OCO) is to prevent the employment of adversary cyberspace capabilities prior to employment. This could mean preemptive action against an adversary.

Office Information System (OIS)
An Office Information System (OIS) is a special purpose Automated Information System (AIS) oriented to word processing, electronic mail, and other similar office functions.

An OIS is normally comprised of one or more

central processing units, control units, storage devices, user terminals, and interfaces to connect these components.

Office of Management and Budget (OMB)
The Federal agency that facilitates budget, policy, legislative, regulatory, and management issues on behalf of the President.

Office of Personnel Management (OPM)
The Office of Personnel Management (OPM) conducts a National Agency Check Plus Written Inquiries (NACI) and Access National Agency Check and Inquiries (ANACI) on Department of Defense (DoD) civilians and a broad range of Personnel Security Investigation (PSI) for other Federal agencies.

NOTE: The OPM is one of the successor agencies to the Civil Service Commission (CSC).

See: Civil Service Commission (CSC)

Office of Special Counsel (OSC)
The Office of Special Counsel (OSC) is an investigative and prosecutorial agency whose basic legislative authority comes from four Federal statutes, the Civil Service Reform Act (CSRA), Whistleblower Protection Act (WBPA), Hatch Act, and the Uniformed Services Employment and Reemployment Rights Act (USERRA). The primary mission of the OSC is the safeguarding of the merit system in Federal employment by protecting employees and applicants from prohibited personnel practices.

The agency also operates a secure channel for Federal whistleblower disclosures of violations of law, rule or regulation; gross mismanagement; gross waste of funds; abuse of authority; and substantial and specific danger to public health and safety.

NOTE: The OSC is one of the successor agencies to the Civil Service Commission (CSC).

See: Civil Service Commission (CSC)

Official Department of Defense Information
All information that is in the custody and control of the Department of Defense (DoD), relates to information in the custody and control of the DoD, or was acquired by DoD employees as part of their official duties or because of their official status within the DoD.

One Time Access
Access granted on a one-time basis to information classified one level higher than that of the current personnel security clearance.

Open Source Information
Information available to the public, including information with limited distribution or access, including information available by subscription.

Open Source Intelligence (OSINT)
Information of potential intelligence value that is available to the general public.

See: Open Source Information

Open Storage Area
The storage of Special Access Program (SAP) material within a Special Access Program Facility (SAPF) in any configuration other than within General Services Administration (GSA)-approved security containers.

Operations and Support
A Special Access Program (SAP) established to protect the planning for, execution of, and support to especially sensitive military operations. An operations and support SAP may protect organizations, property, operational concepts, plans, or activities.

Operations Security (OPSEC)
Process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems; (b) determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

The OPSEC analytical process involves identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Operations Security (OPSEC) Assessment
A thorough evaluation of the effectiveness of a customer's implementation of Operations Security (OPSEC) methodology, resources, and tools.

OPSEC assessments are used to evaluate the effectiveness of the customer's corporate level OPSEC program and can be used at the program level to determine whether or not a program is a viable candidate for an OPSEC survey.

See: Operations Security (OPSEC)

Operations Security (OPSEC) Indicator
Any detectable activity and/or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.

See: Operations Security (OPSEC)

Operations Security (OPSEC) Process
The Operations Security (OPSEC) process is an analytical, risk-based process that incorporates five distinct elements:

- Identifying critical information
- Analyzing threats
- Analyzing vulnerabilities
- Assessing risks; and
- Applying countermeasures.

The OPSEC process examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by potential adversaries.

Operations Security (OPSEC) Program
The vehicle by which the principles and practices of Operations Security (OPSEC) are employed within an organization.

See: Operations Security (OPSEC)

Operations Security (OPSEC) Survey
The application of Operations Security (OPSEC) methodology at the program level.

The OPSEC Survey provides a detailed analysis of all activities associated with a specific operation, project, or program in order to determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.

See: Operations Security (OPSEC)

Operations Security Plan (OSP)
A strategy that analyzes an operation or activity and includes specific Operations Security (OPSEC) measures.

See: Operations Security (OPSEC)

Operations Security Working Group (OWG)
A normally formally designated body representing a broad range of line and staff activities within an organization that provides Operations Security (OPSEC) advice and support to leadership and all elements of the organization.

See: Operations Security (OPSEC)

Optical Storage Media
Optical mass storage devices that are "written" and "read" by light waves (laser), including

compact disks, optical disks, and magneto-optical disks.

Oral/Visual Disclosure
To brief orally, to expose to view, or to permit use under United States (U.S.) supervision in order to permit the transfer of knowledge or information, but not to physically transfer documents, material, or equipment to a foreign government or its representatives.

Organizational-level Commander/Commanding Officer (CO)
The individual, regardless of rank, who has been appointed as the Officer-in-Command of a physical organization.

Original Classification
An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority (OCA)
An individual authorized in writing, either by the United States (U.S.) President, or by agency heads or other officials designated by the President, to classify information in the first instance. OCAs must receive training to perform this duty.

Originating Agency Determination Required (OADR)
Declassification guidance for classified materials. Any material flagged Originating Agency Determination Required (OADR) requires that the agency which originally classified the material

determine whether the information can be declassified.

See: Declassification

Originating Department of Defense (DoD) Component

The Department of Defense (DoD) agency that exercises original classification jurisdiction for classified information.

Outsourced Information Technology-based Process

For Department of Defense (DoD) Information Assurance (IA) purposes, an outsourced Information Technology (IT)-based process is a general term used to refer to outsourced business processes supported by private sector Information Systems (IS), outsourced information technologies, or outsourced information services.

An outsourced IT-based process performs clearly-defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Overseas Security Policy Board (OSPB)

The Overseas Security Policy Board (OSPB), established by the President, considers, develops, coordinates, and promotes policies, standards, and agreements on overseas security operations, programs, and projects that affect all Government agencies under the authority of a Chief of Mission (CM).

Overt Collection
The acquisition of information via the public domain.

Overt Operation
An operation conducted openly without concealment.

Overwrite
A software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data.

Overwriting is an acceptable method for clearing for release to environments of equal classification (TOP SECRET/Special Access Program (SAP) to TOP SECRET/SAP, TOP SECRET/SAP to TOP SECRET/ Sensitive Compartmented Information (SCI)).

NOTE(S): The effectiveness of the overwrite procedure may be reduced by several factors: ineffectiveness of the overwrite procedures; equipment failure (e.g., misalignment of read/ write heads); or inability to overwrite bad sectors or tracks or information in inter-record gaps. Software overwrite routines may also be corrupted by the hostile computer viruses.

Overwriting is not an acceptable method to declassify media.

Overwrite/Re-recording Verification
An approved procedure to review, display, or check the success of an overwrite procedure.

The successful testing and documentation through hardware and random hard-copy readout of the actual overwritten memory sectors.

Parent Corporation
A corporation that owns at least a majority of another corporation's voting securities.

Pass Phrase
Sequence of characters longer than the acceptable length of a password that is transformed by a password system into a virtual password of acceptable length.

Pass/Fail
A declassification technique that regards information at the full document or folder level.

Any exemptible portion of a document or folder may result in failure (exemption) of the entire documents or folders. Documents within exempt folders are exempt from automatic declassification. Documents or folders that contain no exemptible information are passed and therefore declassified.

NOTE: Declassified documents may be subject to Freedom of Information Act (FOIA) exemptions other than the security exemption, and the requirements placed by legal authorities governing Presidential records and materials.

See: Automatic Declassification; Declassification

Password
Protected or private character string used to authenticate an identity or to authorize access to data.

Password Shadowing
The ability with any Operating System (OS) to physically store passwords and/or encrypted password results in a mass storage area of the system other than in the actual password file itself. This feature in intended to prevent the theft of passwords by hackers.

NOTE: Password shadowing is usually a UNIX feature.

See: Password

Perimeter
The perimeter of an Automated Information System (AIS) or network is the extent of the system that is to be accredited as a single system.

Periodic Reinvestigation (PR)
An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation.

The scope consists of a personal interview, National Agency Check (NAC), Local Agency Check (LAC), credit bureau checks, employment records, employment references, and developed character references, and normally will not exceed the most recent 5-year period.

Periods Processing
The processing of various levels of classified or unclassified information at distinctly different times.

NOTE: Under periods processing, the system must be purged of all information from one processing

period before transitioning to the next when there are different users with differing authorizations.

Peripheral
Any devices which are part of an Information System (IS), such as printers, hard and floppy disk drives, and video display terminals.

See: Peripheral Device

Peripheral Device
Any device attached to the network that can store, print, display, or enhance data, such as a disk and/or tape, printer and/or plotter, an optical scanner, a video camera, a punched-card reader, a monitor, or card punch.

See: Peripheral

Permanent Records
Any Federal record that has been determined by the National Archives and Records Administration (NARA) to have sufficient value to warrant its preservation in the National Archives of the United States (U.S.).

Permanent records include all records accessioned by the NARA into the National Archives and later increments of the same records, and those for which the disposition is permanent on Standard Form (SF) 115s, Request for Records Disposition Authority, approved by the NARA on or after May 14, 1973.

Permanent Resident Alien
Any alien lawfully admitted into the United States

(U.S.) under an immigration visa for permanent residence.

See: Alien; Permanent Resident Alien

Personal Computer (PC)
A Personal Computer (PC) is a system based on a microprocessor and comprised of internal memory (Read-Only Memory (ROM) and Random-Access Memory (RAM)), input and/or output, and associated circuitry.

The PC system typically includes one or more read/write devices for removable magnetic storage media (e.g., floppy diskettes, tape cassettes, hard disk cartridges), a keyboard, Cathode Ray Tube or plasma display, and a printer.

Personal Digital Assistant (PDA)
Personal Digital Assistants (PDAs) are mint processors with computing power that are generally smaller than laptop, notebook, or netbook computers.

Personal Financial Statement (PFS)
Form used as part of a personnel security investigation to provide a summary of a person's total monthly income, debt payments, expenses, and the net remainder of income.

Personal Identifiable Information (PII)
Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Personnel Security (PERSEC)
A security discipline that assesses the loyalty, reliability and trustworthiness of individuals for initial and continued eligibility for access to classified information.

Personnel Security Clearance (PCL)
An administrative determination that an individual is eligible, from a security viewpoint, for access to classified information at the same or lower category as the level of the personnel clearance being granted.

Personnel Security Determination
A discretionary security decision by appropriately trained adjudicative personnel of all available personal and professional information that bears on the individual's loyalty to the United States (U.S.), strength of character, trustworthiness, honesty, reliability, discretion and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and the willingness and ability to abide by regulations governing the use, handling, and protection of classified information and/or the execution of responsibilities of a sensitive position.

See: Unfavorable Personnel Security Determination

Personnel Security Interview
An interview conducted with an application for or holder of a security clearance to discuss areas of security relevance. The term is also used to

describe interviews with references in personnel security investigations.

Personnel Security Investigation (PSI)
An investigation required for the purpose of determining the eligibility of Department of Defense (DoD) military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation.

Personnel Security Investigations (PSIs) include investigations of affiliations with subversive organizations, suitability information, or hostage situations, conducted for the purpose of making personnel security determinations. PSIs also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

Personnel Security Program (PSP)
The Department of Defense (DoD) program established to ensure that only loyal, reliable, and trustworthy people are granted access to classified information or allowed to perform sensitive duties.

Personnel Security Questionnaire (PSQ)
Security forms, whether paper or electronic, that

are completed by a subject as part of a Personnel Security Investigation (PSI).

There are three versions of the Personnel Security Questionnaire (PSQ):

1. Standard Form (SF) 85 for Non-Sensitive Positions;
2. SF 85P for Public Trust Positions; and
3. SF 86 for National Security Positions

See: Questionnaire for National Security Positions (QNSP)

Phased Periodic Reinvestigation (PPR)
In September 2005, the Office of Personnel Management (OPM) made the Phased Periodic Reinvestigation (PPR) available as a less comprehensive and less expensive alternative to the Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR). The investigation includes a National Agency Check with Local Agency Checks and Credit Check (NACLC), Personal Subject Interview, and limited reference interviews and record reviews. PPRs may not be requested when certain questions on the clearance application contain responses indicating a possible security or suitability issue.

Physical Damage Assessment
The estimate of the quantitative extent of physical damage based upon observed or interpreted damage.

Physical Security (PHYSEC)
The application of physical barriers and control

procedures as countermeasures against threats to resources and sensitive information. The security discipline concerned with physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Physical Security Waiver
An exemption from specific standards for physical security for Sensitive Compartmented Information Facilities (SCIF) as outlined in Intelligence Community Directive (ICD) 705, "Sensitive Compartmented Information Facilities."

Platform Information Technology (IT) Interconnection
For Department of Defense (DoD) Information Assurance (IA) purposes, platform Information Technology (IT) interconnection refers to network access to platform IT. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric.

Platform IT interconnection has readily identifiable security considerations and needs that must be

addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

Portable Computer System
Any computer system, including Portable Electronic Devices (PEDs) and Portable Computing Devices (PCDs), specifically designed for portability and to be hand carried by an individual.

Examples include grids, laptops, cellular telephones, two-way pagers, palm-sized computing devices, two-way radios with functions including audio, video, data, recording or playback features, personal digital assistants, palmtops, notebooks, data diaries, and watches with communications software and synchronization hardware.

Portable Electronic Device (PED)
Electronic devices having the capacity to store, record, and/or transmit text, images, video, or audio data.

Examples of such devices include pagers, laptops, cellular telephones, radios, compact discs, cassette players and recorders, portable digital assistants, audio devices, watches with input capability, and reminder recorders.

Portfolio
The aggregate of Information Technology (IT) investments for Department of Defense (DoD) Information Systems (IS), infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various assessment and analysis tools to permit information and IT decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions.

Portfolios enable the DoD to manage Information Technology resources and align strategies and programs with DoD-wide, functional, and organizational goals and measures.

Potential Threat
An estimate of the present and future resource allocations and capabilities of an adversary to gain information.

See: Threat Assessment

Preparedness
Actions that involve a combination of planning, resources, training, exercising, and organizing to build, sustain, and improve operational capabilities. It is the process of identifying the personnel, training, and equipment needed for a wide range of potential incidents, and developing jurisdiction-specific plans for delivering capabilities when needed for an incident.

Presidential Historical Materials and Records
The papers or records of former Presidents of the

United States (U.S.) under the legal control of the Archivist pursuant to sections 2107, 2111, 2111note, or 2203 of Title 44, United States Code (U.S.C), as defined at 44 USC 2111, 2111note, and 2001.

Prevention
Actions to avoid an incident or to intervene to stop an incident from occurring.

Prevention involves actions to protect lives and property that may include such countermeasures as: deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Prime Contract
Any contractor who has received a prime contract from a Government agency.

Principal Accrediting Authority (PAA)
The senior official having the authority and responsibility for all Information Systems (IS) within an agency.

Principal Disclosure Authority (PDA)
Oversees compliance with Department of Navy

(DON) disclosure policy and is the only DON official other than the Secretary of the Navy (SECNAV) or Under Secretary of the Navy (UNSECNAV) who is authorized to deal directly with the Secretary or Under Secretary of Defense regarding such matters as DON requests for exceptions to the National Disclosure Policy (NDP).

The PDA for the DON is the Assistant Secretary of the Navy, Research, Development, and Acquisition (ASNRD&A).

Privacy (Not Security)
The rights of an individual or organization to determine for themselves when, how, and to what extent information about them is transmitted to others.

Privacy Data
Any record that is contained in a system of records, as defined in the reference and information the disclosure of which would constitute an unwarranted invasion of personal privacy (DoD Directive 8500.1).

Private Sector
Organizations and entities that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry.

Privileged Access
Explicitly authorized access of a specific user,

process, or computer to a computer resource(s).

Privileged User
The user of an Information System (IS) who has more authority and access to an IS than a general user (e.g., root access, Help Desk support, System Administrator (SA), or an Information Assurance Manager (IAM)/Information Assurance Officer (IAO)).

Profile
A collection and/or display (e.g., a written or graphical description) of the signatures and patterns of an individual or organization.

Program Access Request
A formal request used to nominate an individual for program access.

Program Channels or Program Security Channels
A method or means expressly authorized for the handling or transmission of classified or unclassified Special Access Program (SAP) information whereby the information is provided to indoctrinated persons.

Program Executive Agent
The highest ranking military or civilian individual charged with direct responsibility for the program and who usually appoints the Government Program Manager (GPM).

Program Executive Office, Enterprise Information Systems (PEO-EIS)
The Program Executive Office (PEO), Enterprise

Information Systems is responsible for developing, acquiring, and deploying tactical and non-tactical Information Technology (IT) systems and communications for the Army. Examples include: transportation, medical, personnel, and supply automated tracking and communications systems.

Program Material
Program material and information describing the services provided, the capabilities developed, or the items produced under the Special Access Program (SAP).

Program Office (PO)
The office that manages, executes, and controls a Special Access Program (SAP) in a Department of Defense (DoD) component.

Program Protection
The safeguarding of defense systems and technical data anywhere in the acquisition process, to include the technologies being developed, the support systems (e.g., test and simulation equipment), and research data with military applications. This protection activity involves integrating all security disciplines, counterintelligence, and other defensive methods to protect the essential program information, technologies, and systems data from intelligence collection and unauthorized disclosure.

Program Protection Plan
A comprehensive protection and technology control management tool established for

each defense acquisition program to identify and protect classified and other sensitive information from foreign intelligence collection or unauthorized disclosure.

Program Protection Survey
A survey, conducted during each acquisition phase, to assess the effectiveness of the countermeasures prescribed in the program protection plan at a specific point in time.

Program Security Officer (PSO)
The Government official who administers the security policies for the Special Access Program (SAP).

Program Sensitive Information
Unclassified information that is associated with the program.

Material or information that, while not directly describing the program or aspects of the program, could indirectly disclose the actual nature of the program to a non-program-briefed individual.

Programmable Read-Only Memory (PROM)
A form of digital memory where the setting of each bit is locked by a fuse or antifuse. PROM is used to store programs permanently.

These types of memories are frequently seen in video game consoles, mobile phones, Radio-Frequency Identification (RFID) tags, implantable medical devices, High-Definition Multimedia Interfaces (HDMIs) and in many other consumer and automotive electronics products.

Project/Program Manager (PM)
The single individual responsible for a project or program who manages all daily aspects of the project or program.

Proprietary Information (PROPIN)
Material and information relating to, or associated with, a company's products, business, or activities, including, but not limited to, financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information.

The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

Protected Distribution System (PDS)
A wire line or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Protected Information
Includes sensitive, critical, and/or classified information.

Protection
Actions or measures taken to cover or shield from exposure, injury, or destruction.

Protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities; building resiliency and redundancy; incorporating hazard resistance into initial facility design; initiating active or passive countermeasures; installing security systems; promoting workforce surety, training, and exercises; and implementing cybersecurity measures, among various others.

See: Protective Measures

Protective Measures
Those actions, procedures, or designs implemented to safeguard protected information.

See: Protection

Protective Security Service
A transportation protective service provided by a cleared commercial carrier and qualified by the Military Surface Deployment and Distribution Command (MSDDC) to transport SECRET shipments.

Protocol
Set of rules and formats, semantic and syntactic, that permits entities to exchanged information.

Provider
The contractor, Government support organization, or both, that provides the process on behalf of the customer.

Proxy
Software agent that performs a function or operation on behalf of another application or system while hiding the details involved.

Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

Psychological Operations (PSYOP)
Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals.

The purpose of Psychological Operations (PSYOP) is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Public Domain (PD)
In open view; before the public at large and not in private or employing secrecy or other protective measures.

Public Domain Software (PDS)
Software not protected by copyright laws of any

nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.

Public Information
Official Department of Defense (DoD) information that has been reviewed and approved for public release by the information owner.

Public Key
A value associated with a particular user and used to decrypt messages from that user or encrypt messages to the user. A public key is always associated with a single private key, and can be used to verify digital signatures generated using that private key.
See: Digital Signature; Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)
An enterprise-wide service (i.e., data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption, and digital signature) that supports digital signatures and other public key-based security mechanisms for Department of Defense (DoD) functional enterprise programs, including generation, production, distribution, control, and accounting of public key certificates. A PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are

bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable certification authority.

See: Public Key

Purging

The removal of data from an Information System (IS), its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed.

Note: An IS must be disconnected from any external network before a purge.

See: Sanitization

Questionnaire for National Security Positions (Standard Form 86)
The Standard Form (SF) 86, developed by the Office of Personnel Management (OPM), is used for background investigations (BIs) and reinvestigations. Completed by the applicant, the Questionnaire for National Security Positions provides details on various aspects of the individual's personal and professional background.
See: Personnel Security Questionnaire (PSQ)

Random Procurement
Method of acquiring materials for use in new construction or modification to an existing Sensitive Compartmented Information Facility (SCIF) or secure work area from existing local off-the-shelf stock by TOP SECRET, cleared United States (U.S.) citizens.

Procurement of material will be unannounced, made without referral and immediately transported by the procurer to a Secure Storage Area (SSA). Random procurement may also be used for the acquisition of equipment, material, or supplies to be used in a SCIF or secure area.

Random Selection
The process of selecting a portion of building materials from a bulk shipment, procured for non-specific general construction use.

NOTE: Random selection is not authorized for Sensitive Compartmented Information Facilities (SCIFs) or secure work areas.

Reciprocity
Recognition and acceptance, without further processing of: (1) security background investigations and clearance eligibility determinations; (2) accreditations of information systems; and (3) facility accreditations.

Reciprocity is obligatory in the Intelligence Community (IC) when there are no waivers, conditions, or deviations to the Director of National Intelligence.

Records
The records of an agency and Presidential papers or Presidential records, as those terms are defined in Title 44, United States Code (U.S.C), including those created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

Records Having Permanent Historical Value
Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with Title 44, United States Code (U.S.C).

Records Management
The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Recovery
The development, coordination, and execution of service and site restoration plans; the reconstitution of government operations and services; individual, private sector, nongovernmental, and public assistance programs to provide housing and

to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

Recycled
Recycled is the end state for Information System (IS) storage devices processed in such a way as to make them ready for reuse to adapt them to a new use, or to reclaim constituent materials of value (i.e., smelting).

RED
A designation applied to telecommunications and Information Systems (IS), plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.
See: RED/BLACK Concept

RED Equipment
A term applied to equipment that processes unencrypted National Security Information (NSI) that requires protection during electrical or electronic processing.
See: RED; RED/BLACK Concept

RED Line
An optical fiber or a metallic wire that carries a

RED signal or that originates or terminates in a RED equipment or system.

See: RED; RED/BLACK Concept

RED Optical Fiber Line
An optical fiber that carries a RED signal or that originates or terminates in a RED equipment or system.

See: RED; RED/BLACK Concept

RED Wire Line
A metallic wire that carries a RED signal or that originates or terminates in a RED equipment or system.

See: RED; RED/BLACK Concept

RED/BLACK Concept
Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

Redaction
For purposes of declassification, the removal of exempted information from copies of a document.

Reference
A person other than the subject of a background investigation, identified as having knowledge of the subject. References are characterized by source and type.

There are two sources:

- Listed: The subject of the investigation identified the reference on the Personnel Security Questionnaire.
- Developed: An investigator, in the course of pursuing leads, identified the reference as someone knowledgeable of the subject.

There are six types:

- Education: A faculty member or school administrator at a school attended by the subject who had knowledge of the subject when he or she was a student.
- Employment/Supervisor: A person with management responsibilities for the subject.
- Co-worker: A colleague with knowledge of the subject's on-the-job behavior.
- Neighborhood: A person living in the subject's neighborhood who has knowledge of the subject.
- Friend/Associate: A person who knows the subject socially, preferably away from both work and home.
- Knowledgeable Person: A person who knows the subject in some other context (e.g., a banker or attorney or real estate agent who conducts business on behalf of the subject or a clerk in a store where the subject shops frequently).

NOTE: A specific reference can be categorized as more than one type. For example, someone who is both an office mate and fellow member of a

softball team may be both a co-worker reference and a friend/associate reference.

Reference Material
Documentary material over which the Government Contracting Activity (GCA), who awards the classified contract, does not have classification jurisdiction, and did not have classification jurisdiction at the time the material was originated. Most material made available to contractors by the Defense Technical Information Center (DTIC) and the other secondary distribution agencies is reference material as thus defined.
See: Defense Technical Information Center (DTIC)

Regrade
To raise or lower, as determined appropriate, the classification assigned to an item of information.

Reimbursable Suitability Investigation
Focused investigation to provide additional specific information to resolve developed issues.

Reinstatement
A process whereby a person whose access authorization has been terminated or revoked is permitted to have access to classified information again.

Release
Providing classified information in writing, or any other medium, for retention.
See: Disclosure

Remote Maintenance
An operational procedure that involves connection of a system to an external (e.g., outside of the facility securing the system), remote service for analysis or maintenance.

Remote Terminal
A device for communication with an Automated Information System (AIS) from a location that is not within the central computer facility.

Removable Hard Disk
A hard disk contained in a removable cartridge-type casing.

Report of Investigation (RI)
Report of the results of investigative inquiries. All Personnel Security Investigations (PSIs) and results from criminal and counterintelligence agencies are Reports of Investigation (RI).

Representative of a Foreign Interest
A citizen or national of the United States (U.S.) who is acting as a representative of a foreign government, an agency of a foreign government, or a representative of a foreign government.

Research and Technology
Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity.

Response
Immediate actions to save lives, protect property and the environment, and meet basic human

needs. Response also includes the execution of emergency plans and actions to support short-term recovery.

See: Responsive Force

Response Force
Personnel, not including those on fixed security posts, appropriately equipped and trained, whose duties include initial or follow up response to situations which threaten the security of the Special Access Program Facility (SAPF). This includes local law enforcement support or other external forces as noted in agreements.

See: Response

Restricted Area (RA)
A controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the Cognizant Security Agency (CSA).

Restricted Data (RD)
All data concerning design, manufacture, or utilization of atomic weapons; or, the production of special nuclear material; or, the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under Section

142 of the Atomic Energy Act (AEA) of 1954, as amended.

Revocation
An adjudicative decision to permanently withdraw an individual's clearance(s) based on a personnel security investigation, other relevant information, or both, that a cleared person is no longer eligible for access to classified information.

Revocation of Facility Security Clearance (FCL)
Administrative action that is taken to terminate all classified activity of a contractor because the contractor refuses, is unwilling, or has consistently demonstrated an inability to protect classified information.

Risk
A measure of the potential degree to which protected information is subject to loss through adversary exploitation.
See: Risk Management

Risk Analysis
A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.
See: Risk; Risk Management

Risk Assessment
A written evaluation supporting the adjudicative process, especially when a significant exception to a personnel security standard is being considered.

This assessment should consist of an evaluation from security, counterintelligence, and other technical or management experts as appropriate, and should contrast the compelling national security benefit of an individual accessed to Sensitive Compartmented Information (SCI) with the risk.

See: Risk; Risk Management

Risk Avoidance

A security philosophy which postulates that adversaries are all-knowing and highly competent, against which risks are avoided by maximizing defenses and minimizing vulnerabilities.

See: Risk; Risk Management

Risk Management (RM)

The comparison and analysis of the relative threat (intent and capability to collect the information); the vulnerability of the asset; the cost and administrative burden of possible countermeasures; and the value of the asset used to determine the appropriate level of protection to control and reduce the risk of compromise or disclosure to acceptable levels. Risk management allows the acceptance of risk in the security process based upon a cost-benefit analysis.

See: Risk

Robustness

A characterization of the strength of a security function, mechanism, service, or solution, and the assurance (or confidence) that it is implemented

and functioning correctly.

The Department of Defense (DoD) has three levels of robustness:

- High Robustness: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.
- Medium Robustness: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.
- Basic Robustness: Security services and mechanisms that equate to good commercial practices.

Role-Based Access Control (RBAC)

The identification, authentication, and authorization of individuals based on their job titles or roles and responsibilities within an organization.

See: Discretionary Access Control (DAC); Mandatory Access Control (MAC)

Routine Changes

Changes which have a minimal effect on the overall Transient Electromagnetic Pulse Emanation Standard (TEMPEST) security of the Special Access Program Facility (SAPF). Adding a different type of electronic information processing equipment (unless the equipment added is known to have an unusually large TEMPEST profile), movement of the equipment within the facility, and minor installation changes are examples of routine changes.

Sabotage
The willful destruction of Government property with the intent to cause injury, destruction, defective production of national defense, or war materials by either an act of commission or omission.

Safeguarding
Controls that are prescribed to protect classified information.

Sanitizing
The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.
See: Purging

Scattered Castles
The Intelligence Community (IC) security clearance repository and the Director of National Intelligence's (DNI) authoritative source for clearance and access information for all IC, military services, Department of Defense (DoD) civilians, and contractor personnel.
NOTE: DoD information is furnished by the Joint Personnel Adjudication System (JPAS).
See: Joint Personnel Adjudication System (JPAS)

Scheduled Records
All records that fall under a National Archives and Records Administration (NARA)-approved records control schedule are considered to be scheduled records.

Scope
The time period to be covered and the sources of information to be contacted during the prescribed course of a Personnel Security Investigation (PSI).

Sealed Disk Drive
A fixed hard disk drive in which the heads and platters are encased in the same, sealed unit.
See: Hard Disk

SECRET
The designation applied to classified information which the unauthorized disclosure could reasonably be expected to cause serious damage to national security.

Secure Copy
A computer program which is part of the Computer Security Toolbox.

Secure Copy is a Microsoft Disk Operating System (MS-DOS)-based program used to eliminate appended data within a file or files while transferring the same from a source disk or diskette to a target disk or diskette.
See: Computer Security Toolbox

Secure Data Device (SDD)
Secure Data Devices (SDDs) protect classified

Government data transmissions. SDDs provide Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) secure data transmission functions without voice features and is fully interoperable with all other STU-III/STE products. It allows the user to access a computer database, send a facsimile message, or use email and be sure the information is protected. The SDD was developed under the Government's STU-III/STE program and is approved for use by Federal departments, agencies, and Government contractors.

See: Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE)

Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE)

Telephonic system and associated equipment using a ciphering engine to allow for encrypted transmission of voice and other audio and/or digital data over the public telephone network. Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) operate by taking an audio signal and digitizing it into a serial data stream, usually 8,000 bits per second. This is then mixed with a "keying stream" of data created by an internal ciphering algorithm. This mixed data is then passed through an internal Codec to convert it back to audio so it can be passed over the telephonic system.

NOTE: STU-III/STE is endorsed by the National Security Agency for protecting classified, sensitive, or unclassified United States (U.S.) Government

information, when appropriately keyed.
See: Codec

Secure Working Area
An accredited facility or area that is used for handling, discussing, or processing, but not for storage of Special Access Program (SAP) information.

Security
The protection of information to assure it is not accidentally or intentionally disclosed to unauthorized personnel.

Security Assurance
The written confirmation requested by, and exchanged between governments, of the security clearance level or eligibility for clearance of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of United States (U.S.) classified information possesses the requisite security clearance, is approved by his or her government for access to information of the security classification involved on behalf of the foreign government, and that the recipient will comply with any security requirements specified by the U.S. In the case of contractors, security assurance includes a statement concerning the level of storage capability.

Security Classification Guides Security
Classification Guides are issued for each system, plan, program or project in which classified

information is involved.

Security Clearance
An administrative authorization for access to national security information up to a stated classification level (TOP SECRET, SECRET, CONFIDENTIAL).

NOTE: A security clearance does not, by itself, allow access to controlled access programs.

See: Access Approval; Collateral Information; Controlled Access Program (CAP); Special Access Program (SAP)

Security Cognizance
The Defense Security Service (DSS) office assigned responsibility for the discharge of industrial security responsibilities.

Security Compromise
The disclosure of classified information to persons not authorized access thereto.

Security Countermeasures
Actions, devices, procedures, and/or techniques to reduce security risk.

Security Director (SD)
Senior individual responsible for the overall security management of Special Access Program (SAP) within that activity.

Security Domain
Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties

such as its security classification, security compartment, or sensitivity.

The controls are applied both within an Information System (IS) and in its connection to other classified or unclassified Information Systems.

Security Environment Changes
Changes which have a detrimental effect on the facility. Changes to the inspectable space, addition of a radio transmitter or a modem for external communications, removal or reduction of an existing Transient Electromagnetic Pulse Emanation Standard (TEMPEST) countermeasure (Radio Frequency Interference Shielding, Filters, Control/Inspectable space, etc.) would be changes to the security environment.

Security Environment Threat List (SETL)
A list of countries with United States (U.S.) Diplomatic Missions compiled by the Department of State (DOS) and updated semi-annually.

The listed countries are evaluated based on transnational terrorism; political violence; human intelligence; technical threats; and criminal threats.

The following four threat levels are based on these evaluations:

- Critical: A definite threat to U.S. assets based on an adversary's capability, intent to attack, and targeting conducted on a recurring basis.
- High: A credible threat to U.S. assets based

on knowledge of an adversary's capability, intent to attack, and related incidents at similar facilities.

- Medium: A potential threat to U.S. assets based on knowledge of an adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability to attack through a third party who has demonstrated such a capability.
- Low: Little or no threat as a result of the absence of credible evidence of capability, intent, or history of actual or planned attack against U.S. assets.

Security Incident
A security compromise, infraction, or violation.

Security-in-Depth (SID)
A determination made by the cognizant security agency/authority that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

Security Infraction
A security incident that is not in the best interest of security and does not involve the loss, compromise, or suspected compromise of classified information.

Security Level
A clearance and a set of designators of special

access approval or a classification and a set of such designators, the former applying to a user, the latter applying, for example, to a computer object.

Security Officer
When used alone, includes both Contractor Program Security Officers (CPSOs) and activity security officers at Government facilities.

Security Policy
The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

A complete security policy will necessarily address many concerns beyond the scope of computers and communications.

Security Policy Automation Network (SPAN)
A wide area network (WAN) sponsored by the Office of the Under Secretary of Defense (OUSD) (Policy Support) consisting of a Department of Defense (DoD)-wide SECRET classified network and a separately supported unclassified network that supports communications with foreign among DoD activities on foreign disclosure, export control, and international arms control and cooperation.

Security Policy Board (SPB)
The Board established by the President to consider, coordinate, and recommend policy directives for United States (U.S.) security policies, procedures, and practices.

Security Profile
The approved aggregate of hardware and software and administrative controls used to protect the system.

Security Testing
A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification.

Security Violation
Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; or, any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Executive Order (EO) 13526, "Classified National Security Information," or its implementing directives; or, any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 13526.

Security/Suitability Investigations Index (SSII)
The Office of Personnel Management (OPM) database for personnel security investigations.

Self-Inspection
The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program

established under this order and the implementing directives.

Senior Agency Official (SAO)
The official designated by the agency head to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Senior Foreign Official (SFO)
Any foreign government official who, by virtue of position or access, may directly affect the government's policy. These officials include, but are not limited to: those of ministerial rank and above; the heads of national departments, agencies and services; and representatives of ambassadorial rank and above.

Senior Intelligence Officer (SIO)
The highest-ranking military or civilian individual directly charged with foreign intelligence missions, functions, or responsibilities within a department agency component, command, or element of an Intelligence Community (IC) organization.

Senior Official of the Intelligence Community (SOIC)
The head of an agency, bureau, or intelligence element identified in National Security Act (1947), as amended, 50 United States Code (U.S.C) 401a(4), and Section 3.4(f) (1 through 6) of Executive Order (EO) 12333, "United States Intelligence Activities."

Senior Review Group (SRG)
Provides the principle support to the Special Access Program Oversight Committee (SAPOC). SRG is a "working level" group that reviews all SAPs prior to the SAPOC briefing.

See: Special Access Program Oversight Committee (SAPOC)

Sensitive Activities
Sensitive activities are Special Access (SAPs) or code word programs, critical research and development efforts, operations or intelligence activities, special plans, special activities, or sensitive support to the customer, customer contractors, or clients.

Sensitive Compartmented Information (SCI)
SCI is classified information concerning or derived from intelligence sources and methods or analytical processes that is required to be handled within a formal control system established by the Director of Central Intelligence (DCI).

Sensitive Compartmented Information (SCI) Courier (Certified)
Sensitive Compartmented Information (SCI)-approved active duty military personnel, United States (U.S.) Government civilian employees, or contractor employees whose primary responsibility is to transport SCI material worldwide. The individual is so designated in writing, and must have SCI access approval at the level of material being transported.

See: Sensitive Compartmented Information (SCI) Courier (Designated)

Sensitive Compartmented Information (SCI) Courier (Designated)
Sensitive Compartmented Information (SCI)-approved active duty military personnel, United States (U.S.) Government civilian employees, or contractor employees whose temporary responsibility is to transport SCI material worldwide.

The individual is so designated in writing, and must have SCI access approvals at the level of material being transported.

See: Sensitive Compartmented Information (SCI) Courier (Certified)

Sensitive Compartmented Information Facility (SCIF)
A Sensitive Compartmented Information Facility (SCIF) is an area, room(s), or building installation that is accredited to store, use, discuss, or electronically process Sensitive Compartmented Information (SCI). The standards and procedures for a SCIF are stated in Director of Central Intelligence Directives (DCIDs) 1/19 and 1/21.

Sensitive Compartmented Information Facility (SCIF) (Co-utilization)
The mutual agreement among two or more Government organizations to share the same Sensitive Compartmented Information Facility (SCIF).

Sensitive Compartmented Information Facility (SCIF) Accreditation
Formal acceptance of a Sensitive Compartmented Information Facility (SCIF) as meeting Director of National Intelligence (DNI) security standards and formal authorization to process, store, and/or discuss Sensitive Compartmented Information (SCI).

Sensitive Compartmented Information Facility (SCIF) Database
The Intelligence Community (IC) database that provides a single source listing of Sensitive Compartmented Information Facilities (SCIF) worldwide and is used to promote continuity of operations and relocation of affected resources in the event of a national emergency.

Sensitive Position
Any position so designated within the Department of Defense (DoD), the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on national security.

NOTE: All civilian positions are critical-sensitive, noncritical-sensitive, or non-sensitive.

Sensitivity Label
A collection of information that represents the security level of an object and describes the sensitivity of the data in the object.

A sensitivity label consists of a sensitivity level (classification and compartments) and other

required security markings (e.g., code words, handling caveats) to be used for labeling data.

Service
Honorable active duty (including attendance at the military academies), membership in Reserve Officer Training Corps (ROTC) Scholarship Programs, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a Department of Defense (DoD) contractor or as a consultant involving access under the DoD Industrial Security Program (DISP). Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

Shared Situational Awareness
The comprehensive, cross-network domain knowledge resulting from combining and synthesizing relevant, timely, and comprehensive situational awareness information, tailored to the needs of each organization, which enables a transformational improvement in their ability to operate, maintain, and defend their networks or perform their cybersecurity missions.
See: Situational Awareness

Shipper
One who releases custody of material to a carrier for transportation to a consignee.
See: Consignee, Consignor

Signal Flags
The Intelligence Community (IC) database containing information used to assist security and counterintelligence professionals conducting National Agency Checks (NACs) on individuals applying for positions with IC organizations.

Signals Intelligence (SIGINT)
A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

Significant Derogatory Information
Information that could justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)
A periodic personnel security reinvestigation consisting for TOP SECRET clearances and/ or critical sensitive or special sensitive positions consisting of the elements prescribed in Standard C of Intelligence Community (IC) Policy Guidance 704.1, "Investigative Standards for Background Investigations for Access to Classified Information." Initiated at any time following the completion of, but not later than 5 years, from the date of the previous investigation or reinvestigation.

Single Scope Background Investigation (SSBI)
The only Personnel Security Investigation (PSI)

conducted by Defense Security Service (DSS) for the Department of Defense (DoD) Personnel Security Program (PSP) for TOP SECRET and Sensitive Compartmented Information (SCI) duties.

The period of investigation for a Single Scope Background Investigation (SSBI) is variable, ranging from 3 years for neighborhood checks to 10 years for Local Agency Checks (LACs).

Site Information Assurance Manager (IAM)
The single Information Systems (IS) security focal point for a defined site.

The Site Information Assurance Manager (IAM) supports two organizations: User Organization and Technical Organization, and is responsible for managing the baseline and ensuring that changes to the site baseline are properly controlled.

Site Security Manager (SSM) (Construction)
A United States (U.S.) citizen, at least 18 years of age, cleared at the TOP SECRET level and approved for Sensitive Compartmented Information (SCI), and is responsible for security where a Sensitive Compartmented Information Facility (SCIF) is under construction.

Situational Awareness
The knowledge and understanding of the current operational status, risk posture, and threats to the cyber environment gained through instrumentation, reporting, assessments, research, investigation, and analysis, which are used to enable well-informed decisions and timely actions

to preempt, deter, defend, defeat, or otherwise mitigate those threats and vulnerabilities.

See: Shared Situational Awareness

Sole Proprietorship
A business owned by one individual who is liable for the debts and other liabilities incurred in the operation of the business.

Sound Attenuation
Diminution of the intensity of sound energy propagating in a medium, caused by absorption, spreading, and scattering.

Sound Group
Voice transmission attenuation groups established to satisfy acoustical requirements.

Ratings measured in sound transmission class may be found in the Architectural Graphic Standards (AGS).

See: Sound Attenuation

Sound Masking System
An electronic system used to create background noise to mask conversations and counter audio-surveillance threats.

Sound Transmission Class
The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.

Source Document
An existing document that contains classified

information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP)
A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Special Access Program (SAP)/Special Access Required (SAR)
Any program imposing Need-to-Know or access control beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine Need-to-Know; or special lists of persons determined to have a Need-to-Know.

See: Need-to-Know

Special Access Program Central Office (SAPCO)
Office under the Department of Defense (DoD), Office of the Secretary of Defense (OSD), or the military department responsible for establishment and application of regulations, oversight, and security policy for Special Access Programs (SAPs).

See: Special Access Program Coordination Office (SAPCO)

Special Access Program Coordination Office (SAPCO)
Office under the Department of Defense (DoD), or the military department components responsible for establishment and application of regulations, oversight, and security policy for Special Access Programs (SAPs).

See: Special Access Program Central Office (SAPCO)

Special Access Program Facility (SAPF)
A specific physical space that has been formally accredited in writing by the cognizant Program Security Officer (PSO) which satisfies the criteria for generating, safeguarding, handling, discussing, and storing classified or unclassified program information, hardware, and materials.

Special Activity
An activity or associated support function conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the Government is neither apparent nor acknowledged publicly.

Special activities are not intended to influence United States (U.S.) political processes, public opinion, policies, or media, and do not include diplomatic activities or the collection and production of intelligence or related support functions.

Special Background Investigation (SBI)
A Personnel Security Investigation (PSI) consisting

of all the components of a Background Investigation plus certain additional investigative requirements. The period of investigation for a Special Background Investigation (SBI) is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Special Investigative Inquiry (SII)
A supplemental Personnel Security Investigation (PSI) of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination.

Special Program Document Control Center
The component's activity assigned responsibility by the Information System Security Representative (SSR) for the management, control, and accounting of all documents and magnetic media received or generated as a result of the special program activity.

Special Program Review Group (SPRG)
The committee responsible for developing the Air Force Special Access Required (SAR) programs resource requirements, including the Program Objective Memorandum (POM), Budget Estimate Submission (BES), and the President's Budget.

Special Security Center (SSC) The Director of National Intelligence (DNI) element responsible for developing, coordinating, and overseeing DNI security policies and databases to support Intelligence Community security elements. The Special Security Center (SSC) interacts with other Intelligence Community (IC) security organizations to ensure that DNI equities are considered in the development of national level security policies and procedures.

Sponsoring Agency
A Government department or agency that has granted access to classified national intelligence, including Sensitive Compartmented Information (SCI), to a person whom it does not directly employ, e.g., a member of another Government organization or a contractor employee.

Stand-Alone Automated Information System (AIS)
A stand-alone Automated Information System (AIS) may include desktop, laptop, and notebook personal computers, and any other hand-held electronic device containing classified information.

NOTE: Stand-alone AIS by definition are not connected to any Local Area Network (LAN) or other type of network.

See: Stand-Alone System

Stand-Alone System
An Information System (IS) operating independent

of any other IS within an environment physically secured commensurate with the highest classification of material processed or stored thereon.

See: Stand-Alone Automated Information System (AIS)

Standard Practice Procedures
A document(s) prepared by a contractor that implements the applicable requirements of the DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," for the contractor's operations and involvement with classified information at the contractor's facility.

Statement of Reason (SOR)
A letter from a Central Adjudication Facility (CAF) to a subject, notifying of the CAF's intent to deny or revoke security clearance or eligibility, and the reasons for the proposed action.

Static Random-Access Memory (SRAM)
A read-write Random-Access Memory (RAM) that uses either four transistors or two resistors to form a passive-load flip-flop, or six transistors to form a flip-flop with dynamic loads for each cell in an array.

Once data is loaded into the flip-flop storage elements, the flip-flop will indefinitely remain in that state until the information is intentionally changed or the power to the memory circuit is shut off.

See: Dynamic Random-Access Memory (DRAM); Ferroelectric Random-Access Memory (FRAM)

Subcontract
A contract entered into by a contractor to furnish supplies or services for performance of a prime contract or other subcontract.

See: Subcontractor

Subcontractor
A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a Prime Contractor.

Subject Matter Expert (SME)
An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team.

Subsidiary
A corporation in which another corporation owns at least a majority of its voting securities.

Substantial Issue Information
Any information or aggregate of information that raises a significant question about the prudence of granting access eligibility.

NOTE: Substantial issue information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility.

See: Issue Information (Personnel Security); Minor Issue Information

Supporting Information Assurance (IA) Infrastructure
Collection of interrelated processes, systems, and networks that provide a continual flow of

information assurance services throughout the Department of Defense (DoD) (e.g., the key management infrastructure or the incident detection and response infrastructure).

Surface Deployment and Distribution Command (SDDC)
A major command of the United States (U.S.) Army, and the U.S. Transportation Command's (TRANSCOM) component command responsible for designated domestic land transportation as well as common-user water terminal and traffic management service to deploy, employ, sustain, and redeploy U.S. forces on a global basis.

Surreptitious Entry
Unauthorized entry in a manner which leaves no readily discernible evidence.

Surveillance
The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, photographic, or other means.

Survivability
The capability of a system to withstand a man-made or natural hostile environment without suffering an abortive impairment of its ability to accomplish its dedicated mission.

Suspicious Contact
Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared

employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

System
An assembly of computer and/or communications hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

System Administrator (SA)
The individual responsible for maintaining the system in daily operations.

The System Administrator (SA) has responsibility to:

- Manage system hardware and software, data storage devices, and application software
- Manage system performance
- Provide system security and customer support
- Perform equipment custodian duties
- Maintain software licenses and documentation
- Monitor hardware and software maintenance contracts
- Establish User IDs and passwords
- Ensure adequate network connectivity

- Review audit trails
- Provide backup of systems operations and other system unique requirements

See: Information Assurance Officer (IAO)

System Security Authorization Agreement (SSAA)
A formal document that fully describes the planned security tasks required to meet system or network security requirements. The package must contain all information necessary to allow the Designated Approving Authority (DAA) to make an official management determination for authorization for a system or site to operate in a particular security mode of operation; with a prescribed set of safeguards; against a defined threat with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnections to external systems; and at an acceptable level of risk.

System Security Engineering (SSE)
The efforts to help achieve maximum security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort.

System Security Plan (SSP)
Formal document that provides an overview of the security requirements for the information system and describes the security controls in place

or planned for meeting those requirements.

See: System Security Authorization Agreement (SSAA)

System Software

Computer programs that control, monitor, or facilitate use of the Information System (IS) (e.g., operating systems, programming languages, communication, input-output control, sorts, security packages and other utility-type programs). Also includes off-the-shelf application packages obtained from manufacturers and commercial vendors, such as word processing, spreadsheets, database management, graphics, and computer-aided design.

Systematic Declassification Review

The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with Title 44, United States Code (U.S.C), Section 2103.

Tactical Approval to Operate (T-ATO)
Cognizant Security Authority (CSA)-delegated authority to an operational element to allow a Tactical Sensitive Compartmented Information Facility (T-SCIF) to be functional before formal accreditation is received.

NOTE: The Tactical Approval to Operate (T-ATO) may not exceed one year in duration.

Tactical Sensitive Compartmented Information Facility (T-SCIF)
An area, room, group of rooms, building, or installation accredited for Sensitive Compartmented Information (SCI)-level processing, storage, and discussion that is used for operational exigencies (actual or simulated) for a specified period of time not exceeding 1 year.

Tactical Special Access Program Facility (T-SAPF)
An accredited area used for actual or simulated war operations for a specified period of time.

Target
An individual, operation, or activity which an adversary has determined possesses information that might prove useful in attaining his or her objective.

Tear Line
A place in an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified or controlled report begins.

The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination in accordance with the Need-to-Know, need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.

Technical Data
Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation. Specific examples include: Classified information relating to defense articles and services; information covered by an invention secrecy order; and software directly related to defense articles.

NOTE: This definition does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

Technical Security
A security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies.

The discipline mandates training in various countermeasure techniques.

Technical Surveillance Countermeasures (TSCM)
Physical, electronic, and visual techniques used to detect and counter technical surveillance devices, technical security hazards, and related physical security deficiencies.
See: Countermeasure (CM)

Technical Surveillance Countermeasures (TSCM) Inspection
A Government-sponsored comprehensive physical and electronic examination of an area by trained and specially equipped security personnel to detect or counter technical surveillance penetrations or hazards.
See: Technical Surveillance Countermeasures (TSCM)

Technical Surveillance Countermeasures (TSCM) Surveys and Evaluations
A physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration.
See: Technical Surveillance Countermeasures (TSCM)

Technical Threat Analysis
A continual process of compiling and examining all available information concerning potential technical surveillance activities by intelligence collection groups which could target personnel,

information, operations and resources.

Technical Vulnerability
A hardware, firmware, communication, or software weakness which leaves an Information System (IS) open for potential exploitation or damage, either externally resulting in risk for the owner, user, or manager of the IS.

Technology
The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves, or the technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software.

Technology Control Plan (TCP)
The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and protective measures as necessary to protect the United States (U.S.) technological or operational advantage represented by the system.

Technology Critical
Technologies that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (U.S.), consisting of:

- Arrays of design and manufacturing know-how, including technical data
- Keystone manufacturing, inspection, and test equipment
- Keystone materials
- Goods accompanied by sophisticated operation, application, or maintenance know-how

NOTE: Also referred to as Militarily Critical Technology (MCT).

Technology Transfer
Transferring, exporting, or disclosing defense articles, defense services, or defense technical data covered by the United States Munitions List (USML) to any foreign person or entity in the United States (U.S.) or abroad.

Telecommunications
Preparation, transmission, communication or related processing of information (e.g., writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and Automated Information Systems Security (TISS)
Superseded by Information Systems Security (INFOSEC).

Telemetry
The science and technology of automatic data measurement and transmission, as by wire or radio, from remote sources, such as space vehicles, to a receiving station for recording and analysis.

Telemetry Intelligence (TELINT)
Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry. Telemetry Intelligence (TELINT) is a subcategory of Foreign Instrumentation Signals Intelligence (FISINT).

See: Foreign Instrumentation Signals Intelligence (FISINT)

Telework
Any arrangement in which an employee performs officially assigned duties at an alternative worksite on a regular, recurring, or ad hoc basis, not including while on official travel.

Temporary Access Eligibility
Access based on the completion of minimum investigative requirements under exceptional circumstances where official functions must be performed prior to completion of the investigation and adjudication process. Temporary eligibility for

access may be granted before the investigations are complete and favorably adjudicated. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

See: Interim Access Authorization (IAA); Interim Security Clearance

Temporary Help/Job Shopper
An individual employed by a cleared company whose services are retained by another cleared company or Government activity performing on Special Access Program (SAP) contracts and providing required services (e.g. computer, engineering, administrative support, etc.) under a classified contractual agreement. This individual will have access to SAP material only at locations designated by the utilizing activity.

Temporary Records
Federal records approved for disposal, either immediately or after a specified retention period.

See: Disposable Records

Terrorism
The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Threat
Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DOS).

Threat Analysis
An Operations Security (OPSEC) process which examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

See: Threat Assessment

Threat Assessment
An evaluation of the intelligence collection threat to a program activity, system, or operation.

See: Threat Analysis

Threat Monitoring
The analysis, assessment, and review of Information System (IS) audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of data or system security.

Toluene
A colorless, flammable, aromatic liquid obtained from coal tar or petroleum and used in some fuels, dyes, and explosives. Toluene is also used as a solvent/thinner for some gums, lacquers, and

paints and is also called Xylene or Methylbenzene. These markers tend to be strong smelling and may damage Compact Discs (CDs)/Digital Video Discs (DVDs).

TOP SECRET
The designation applied to information of which the unauthorized disclosure of could reasonably be expected to cause exceptionally grave damage to national security.

Transferred Records
Records transferred to Agency storage facilities or a Federal records center.

Transient Electromagnetic Pulse Emanation Standard (TEMPEST)
The investigation, study, and control of compromising emanations from telecommunications and Information Systems (IS) equipment.

Transient Electromagnetic Pulse Emanation Standard (TEMPEST)
Certified Equipment/System Equipment or systems that have complied with the national requirements of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92 Level I or previous editions.

Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone
A defined area within a facility where equipment

with appropriate Transient Electromagnetic Pulse Emanation Standard (TEMPEST) characteristics (TEMPEST zone assignment) may be operated with emanating electromagnetic radiation beyond the controlled space boundary of the facility.

See: Equipment Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone (ETZ); Facility Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone (FTZ)

Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zoned Equipment
Equipment that has been evaluated and assigned an equipment zone corresponding to the level in National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92.

This equipment must be installed according to the NSTISSAM and Headquarters (HQ)-Level specialized installation instructions.

Transmission
The sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Transmission Security (TRANSEC)
The component of Communications Security

(COMSEC) that results from all measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.

Transportation Plan
A comprehensive plan covering the movement of classified material between participants of an international program or project.

Transshipping Activity
A Government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

Trapdoor
Operating System (OS) and applications that usually have safeguards to prevent unauthorized personnel from accessing or modifying programs.

Trigraph
A three-letter acronym for the assigned code word or nickname.
See: Digraph

Trojan Horse
A computer program with an apparently or actually useful function that contains additional or hidden functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (e.g., making a "blind copy" of a sensitive file for the creator of the Trojan Horse).
See: Malicious Code

Trusted Computer System (TCS)
A system that employs sufficient hardware and software integrity measures to allow its use for processing sensitive or classified information.

Trusted Computing Base (TCB)
The totality of protection mechanisms with a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy.

NOTE: The ability of a Trusted Computing Base (TCB) to correctly enforce a unified security policy depends on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

Trusted Path
A mechanism by which a person at a terminal can communicate directly with the trusted computing base. This mechanism can only be activated by the person or the trusted computing base and cannot be imitated by untrusted software.

Two-Person Integrity
A provision that prohibits one person from working alone.

Type 1 Products
Classified or controlled cryptographic items endorsed by the National Security Agency (NSA) for securing classified and sensitive United States (U.S.) Government information, when

appropriately keyed.

The term refers only to products, and not to information, keys, services, or controls. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulations (ITAR).

Type Accepted Telephone

Any telephone whose design and construction conforms to the design standards for Telephone Security Group (TSG)-approved telephone sets.

Umbrella Special Access Program (SAP)
An approved Department of Defense (DoD) Special Access Program (SAP) that contains compartments for specific projects within the overall program. While there is no formal requirement to obtain separate approval for each individual project under the umbrella SAP, each project must be consistent with the Special Access Program Oversight Committee (SAPOC)-approved scope of the umbrella SAP. The nickname, program description, and accomplishments of each significant project will be reported in the annual Special Access Program report.
NOTE: An individual participant's access can be afforded across-the-board at the umbrella level or specific individual project access can be granted on a limited or non-umbrella level.

Unacknowledged Special Access Program (SAP)
The existence of the Special Access Program (SAP) is protected as special access and the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is often unacknowledged, classified, or not directly linked to the program. The four Congressional Defense Committees normally have access to the unacknowledged SAP.

Unauthorized Disclosure (UD)
A communication or physical transfer of classified information to an unauthorized recipient.

Unauthorized Person
A person not authorized to have access to specific classified information.

Unclassified Controlled Nuclear Information (UCNI)
Unclassified Controlled Nuclear Information (UCNI) under jurisdiction of the Department of Energy (DOE) includes unclassified facility design information, operational information concerning the production, processing, or utilization of nuclear material for atomic energy defense programs, safeguards and security information, nuclear material, and declassified controlled nuclear weapon information once classified as Restricted Data (RD). Department of Defense (DoD) UCNI is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities. Information is designated UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of SNM, equipment, or facilities.

Unclassified Internet Protocol Router Network
Used to exchange sensitive but unclassified information between "internal" users as well as

providing users access to the Internet.

The Unclassified Internet Protocol Router Network is composed of Internet Protocol routers owned by the United States Department of Defense (DoD). It was created by the Defense Information Systems Agency (DISA) to supersede the earlier Military Network.

See: Non-Secure Internet Protocol Router Network (NIPRNET)

Unclassified Sensitive

For computer applications, this term refers to any information, which the loss, misuse, unauthorized access to, or modification of could adversely affect the national interest or the conduct of a Federal program, or the privacy to which individuals are entitled under the section 552a of Title 5, United States Code (U.S.C), "Privacy Act," but which has not been specifically authorized under the criteria established by an Executive Order (EO) or an act of Congress to be kept secret in the interest of national defense or foreign policy.

See: Computer Security Act; Sensitive but Unclassified Information

Uncontrolled Access Area (UAA)

The space in and around a building where no personnel access controls are exercised.

Undercover Operation

A phrase usually associated with the law enforcement community and which describes an operation that is so planned and executed as to

conceal the identity of, or permit plausible denial by, the sponsor.

Unfavorable Administrative Action
Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations.

Unfavorable Personnel Security Determination
Any one or a combination of the following scenarios:

- Denial/revocation of clearance for access to classified information
- Denial/revocation of access to classified information
- Denial/revocation of a Special Access Authorization (AA), including access to Sensitive Compartmented Information (SCI)
- Non-appointment/non-selection for appointment to a sensitive position
- Non-appointment/non-selection for any other position requiring trustworthiness
- Reassignment to a position of lesser sensitivity or to a non-sensitive position
- Non-acceptance for or discharge for the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance

See: Personnel Security Determination

Unified Network
A connected collection of systems or networks that are accredited under a single System Security Plan (SSP); as a single entity; and by a single Cognizant Security Authority (CSA). A unified network can be as simple as a small standalone Local Area Network (LAN) operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single Information System Security Officer (ISSO). The network can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy accredited as a single CSA. The perimeter of each network encompasses all its hardware, software, and attached devices, and its boundary extends to all of its users.

United States (U.S)
The 50 states and the District of Columbia (D.C.).

United States (U.S) and its Territorial Areas
The 50 states, the District of Columbia (D.C.), Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.

United States (U.S) Citizen (Native-Born)
A person born in one of the 50 United States (U.S.), Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands, or Panama Canal Zone, if the father, mother, or both, was or is

a citizen of the U.S.

United States (U.S) National
A citizen of the United States (U.S.) or a person who, though not a citizen of the U.S., owes permanent allegiance to the U.S. (e.g., a lawful permanent resident of the U.S.). Categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. are listed in 8 United States Code 1101(a) and 8 United States Code 1401; subsection (a) paragraphs (1) through (7). Legal counsel should be consulted when doubt exists as to whether or not a person can qualify as a national of the United States.

NOTE: A U.S. national shall not be treated as a foreign person except when acting as a foreign representative.

United States Computer Emergency Readiness Team (US-CERT)
The Department of Homeland Security (DHS United States Computer Emergency Readiness Team (US-CERT) is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

United States Cyber Command (USCYBERCOM)
The United States Cyber Command (USCYBERCOM) plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department

of Defense (DoD) information networks and to prepare to (and when directed) conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure freedom of action in cyberspace for the United States (U.S.) and its allies, and deny the same to adversaries.

USCYBERCOM is a subordinate command of the United States Strategic Command (USSTRATCOM).

See: United States Strategic Command (USSTRATCOM)

United States Strategic Command (USSTRATCOM)
The United States Strategic Command (USSTRATCOM) directs the operation and defense of the Global Information Grid (GIG) to assure timely and secure net-centric capabilities across strategic, operational, and tactical boundaries in support of the Department of Defense's (DoD) full spectrum of warfighting, intelligence, and business missions.

See: Global Information Grid (GIG)

Unscheduled Records
Federal records whose final disposition has not been approved.

Upgrade
A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

User Identification
A unique symbol or character string that is used by an Information System (IS) to uniquely identify a specific user.

Users
Any person who interacts directly with an Automated Information System (AIS) or a network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (e.g., active/passive wiretapping).

Vault
A room(s) used for the storing, handling, discussing, and/or processing of Special Access Program (SAP) information and constructed to afford maximum protection against unauthorized entry.

Vendor
The manufacturer or sellers of the Automated Information System (AIS) equipment and/or software used on the special program.

Violation
Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; or, any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Executive Order (EO) 13526, "Classified National Security Information," or its implementing directives; or, any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 13526.

Virus
A malicious computer program that is designed to replicate itself by copying itself into the other programs stored in a computer. The intent of the virus is varying levels of negative effects, such as causing a program to operate incorrectly or corrupting a computer's memory.
See: Malicious Code

Volatile Memory
Computer memory that does not retain data after removal of all electrical power sources and/or when reinserted into a similarly configured Automated Information System (AIS). In contrast to Non-Volatile Memory (NVM), volatile memory retains data as long as the power supply is on, but if the power supply is removed or interrupted, the stored memory is lost.

See: Non-Volatile Memory (NVM); Non-Volatile Random-Access Memory (NVRAM)

Voting Securities
Any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

Vulnerability
A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Analysis
A process which examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.

See: Vulnerability Assessment

Vulnerability Assessment
The results of a vulnerability analysis expressed as a degree of probable exploitation by an adversary.
See: Vulnerability Analysis

Waived Special Access Program (SAP)
An unacknowledged Special Access Program (SAP) to which access is extremely limited in accordance with the statutory authority of Section 119e of 10 United States Code (U.S.C), Reference b. The unacknowledged SAP protections also apply to Waived SAPs. Only the Chairman, Senior Minority member, and, by agreement, their Staff Directors of the four Congressional Defense Committees normally have access to program material.

See: Unacknowledged Special Access Program (SAP)

Waiver
An exemption from a specific requirement.

Waiver (Personnel Security)
Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access.

See: Condition (Personnel Security), Deviation (Personnel Security); Exception (Personnel Security)

Weapons of Mass Destruction (WMD)
Chemical, Biological, Radiological, Nuclear, and High-Explosive (CBRNE) weapons capable of a high order of destruction and/or causing mass casualties.

Wide Area Network (WAN)
A computer network that services a large area. Wide Area Networks (WANs) typically span large

areas (e.g., states, counties, or continents), and are owned by multiple organizations.

See: Local Area Network (LAN), Network.

Working Paper(s)

A draft classified document, portion of a classified document, or material accumulated or created while preparing a finished document.

Workstation

A high-performance, microprocessor-based platform that uses specialized software applicable to the work environment.

Worm

A worm is a program, originally developed by systems programmers, which allows the user to tap unused network resources to run large computer programs. The worm would search the network for idle computing resources and use them to execute a program in small segments. Built-in mechanisms would be responsible for maintaining the worm, the worm, finding free machines, and replicating the program. Worms can tie up all the computing resources on a network and essentially shut it down. A worm is normally activated every time the system is booted up.

NOTE: This is differentiated from the acronym WORM (Write-Once, Read Many) descriptive of optical Compact Disk (CD)/Digital Video Disk (DVD) media with single write capability.

See: Malicious Code; Virus

Write-Protect
A term used to indicate that there is a machine hardware capability which may be manually used to protect some storage media from accidental or unintentional overwrite by inhibiting the write capability of the system.

XYZ

Acronyms

A

A/M	Amperes per Meter Units
AA&E	Arms, Ammunition, and Explosives
AAA	Access Approval Authority
AAA	Army Audit Agency
AAR	After-Action Report
ABCS	Army Battle Command System
AC	Alternating Current
ACA	Access Control Authority
ACADA	Automatic Chemical Agent Detector Alarm
ACCF	Army Central Clearance Facility
ACCM	Alternative Compensatory Control Measure
ACDA	U.S. Arms Control and Disarmament Agency
ACERT	Army Computer Emergency Response Team
ACES	Automated Continuing Evaluation System
ACO	Administrative Contracting Officer
ACPG	Advanced Chemical Protective Garment
ACS	Assistant Chief of Staff
ACSI	Assistant Chief of Staff for Intelligence (Army)
ADP	Automated Data Processing
ADPSO	Automated Data Processing Security Officer
ADPSSO	Automated Data Processing System Security Officer
ADR	Adjudicative Desk Reference
ADS	Automated Data System
AEA	Atomic Energy Act
AECA	Arms Export Control Act

AF	Air Force
AFB	Air Force Base
AFC	Agreement for Cooperation
AFCAF	Air Force Central Adjudication Facility
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFOSF	Air Force Office of Security Forces
AFOSI	Air Force Office of Special Investigations
AFOSP	Air Force Office of Security Police
AFPC	Air Force Personnel Center
AFPD	Air Force Policy Directive
AFR	Air Force Regulation
AFSCO	Air Force Security Clearance Office
AG/SCM	Advisory Group/Security Countermeasures
AGS	Architectural Graphic Standards
AHC	Ad Hoc Committee
AHG	Ad Hoc Group
AIA	Aerospace Industries Association
AIA	Air Intelligence Agency
AIA	Army Intelligence Agency
AID	Agency for International Development
AIQC	Antiterrorism Instructor Qualification Course
AIS	Automated Information Systems
AISS	Automated Information Systems Security
AISSP	Automated Information Systems Security Plan
ALASAT	Air-Launched Anti-Satellite Weapon
ALBM	Air-Launched Ballistic Missile

ALCM	Air-Launched Cruise Missile
ALMC	Army Logistics Management College
AM	Amplitude-Modulated
AMCIT	American Citizen
AMP	Amended Mines Protocol
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ANACI	Access National Agency Check with Written Inquiries
AO	Area of Operations
AOA	Analysis of Alternatives
AOA	Area of Application
AOS	Active Overflight System
AP	Armor Piercing
APC	Armored Personnel Carrier
APL	Antipersonnel Landmine
APM	Antipersonnel Mine
AQ-SAP	Acquisition Special Access Program
AR	Army Regulation
ARM	Anti-Radiation Missile
ARTY	Artillery
ASAT	Anti-Satellite Weapon
ASATS	Army Special Access Tracking System
ASBM	Air-to-Surface Ballistic Missile
ASD	Assistant Secretary of Defense
ASEP	Army SAP Enterprise Portal
ASIS	American Society for Industrial Security
ASM	Air-to-Surface Missile
ASNRD&A	Assistant Secretary of the Navy, Research, Development, and Acquisition

ASP	Accredited Security Parameters
ASP	Ammunition Supply Point
ASPO	Acquisition Systems Protection Office
ASPP	Acquisition System Protection Program
ASPWG	Acquisition Systems Protection Working Group
ASSIST	Automated Systems Security Incident Support Team
AT	Anti-Tamper
AT	Assessment/Assistance/ Advance Team
AT/FP	Antiterrorism/Force Protection
ATEA	Anti-Tamper Executive Agent
ATL	Assessment/Assistance/ Advance Team Leader
ATO	Approval to Operate
ATOMAL	North Atlantic Treaty Organization (NATO) Marking for United States (U.S.)/ United Kingdom (UK) Atomic Information
ATTU	Atlantic to the Urals
AUB	Agency Use Block
AVLB	Armored Vehicle Launch Bridge
AWG	American Wire Gauge

B

BACTO	Biological Arms Control Treaty Office
BAT	Base Assistance Team
BCE	Baseline Cost Estimate
BDA	Bilateral Destruction Agreement

BDI	Ballistic Defense Initiative
BDS	Biological Detection System
BES	Budget Estimate Submission
BI	Background Investigation
BIC	Bilateral Implementation Commission
BIDS	Biological Integrated Detection System
BINAS	Biosafety Information Network Advisory System
BIOS	Basic Input-Output System
BIPN	Background Investigation plus Current National Agency Check
BIPR	Periodic Reinvestigation of Background Investigation
BIR	Background Investigation Requested
BIS	Bureau of Industry and Security
BISS	Base and Installation Security System
BITN	Background Investigation (10-Year Scope)
BL	Bill of Lading
BL	Biosafety Level
BM	Ballistic Missile
BMD	Ballistic Missile Defense
BMDO	Ballistic Missile Defense Organization
BMLNA	Ballistic Missile Launch Notification Agreement
BMS	Balanced Magnetic Switch
BOG	Board of Governors
BPAC	Budget Program Activity Code
BPPBS	Biennial Planning, Programming, and Budgeting System

BSA	Bank Secrecy Act
BSDS	Biological Standoff Detection System
BSL	Biological Safety Level
BT	Battle Tank
BTO	Barbed-Tape Obstacle
BTW	Biological and Toxin Weapons
BTWC	Biological and Toxin Weapons Convention
BW	Biological Warfare/Weapons
BWC	Biological Weapons Convention
BXA	Bureau of Export Administration

C

C or E	Conversion or Elimination
C&A	Certification and Accreditation
C2	Command and Control
C2W	Command and Control Warfare
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
CAA	Controlled Access Area
CAB	Civil Aeronautics Board
CAEST	Conventional Armaments and Equipment Subject to the Treaty
CAF	Central Adjudication Facility
CAGE	Commercial and Government Entity

CAM	Chemical Agent Monitor
CAMDS	Chemical Agent Munitions Disposal System
CAMIN	Chemical Accountability Management and Information Network
CAN	Computer Network Attack
CAO	Contract Administration Office
CAP	Controlled Access Program
CAPCO	Controlled Access Program Coordination Office
CAPDS	Chemical Agent Point Detection System
CAPOC	Controlled Access Program Oversight Committee
CARDS	Chemical Agent Remote Detection System
CAS	Chemical Abstracts Service
CAS	Collaborative Adjudicative Services
CB	Citizen's Band
CBD	Chemical Biological Defense
CBDE	Chemical and Biological Defense Equipment
CBDP	Chemical Biological Defense Program
CBI	Confidential Business Information
CBIPM	Confidential Business Information Protective Measure
CBM	Confidence-Building Measure
CBO	Congressional Budget Office
CBR	Chemical, Biological, and Radiological

CBRD	Chemical, Biological, and Radiological Defense
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Explosive
CBW	Chemical and Biological Warfare/ Weapons
CBX	Computerized Branch Exchange
CC	Chain of Command
CC	Component Commander
CCB	Community Counterterrorism Board
CCB	Configuration Control Board
CCD	Conference of the Committee on Disarmament
CCI	Controlled Cryptographic Item
CCIR	Commander's Critical Information Requirements
CCISCMO	Community Counterintelligence, and Security Countermeasures Office
CCL	Commerce Control List
CCM	Classification and Control Markings
CCMS	Case Control Management System
CCT	Case Closing Transmittal
CCTV	Closed-Circuit Television
CCVS	Central Clearance Verification System
CCW	Convention on Conventional Weapons
CD	Compact Disk
CD	Conference on Disarmament
CDC	Centers for Disease Control and Prevention

CDC	Cleared Defense Contractor
CDF	Chemical Agent Disposal Facility
CDR	Commander
CDR	Critical Design Review
CD-R	Compact Disk-Read
CD-ROM	Compact-Disk, Read-Only Memory
CDSE	Center for Development of Security Excellence
CDTF	Chemical Defense Training Facility
CE	Compromising Emanations
CEP	Continuous Evaluation Program
CERT	Committee of Emergency Response Team
CERT	Computer Emergency Response Team
CFE	Conventional Armed Forces in Europe Treaty
CFIUS	Committee on Foreign Investment in the United States
CFR	Code of Federal Regulations
CG	Command Guidance
CI	Character Investigation
CI	Counterintelligence
CI	Critical Information
CIA	Central Intelligence Agency
CIAR	Counterintelligence Awareness and Reporting
CID	Criminal Investigation Division
CIDC	Criminal Investigation Division Command (Army)

CIFA	Counterintelligence Field Activity
CIIA	Critical Infrastructure Information Act
CIK	Crypto-Ignition Key
CINC	Command-in-Chief
CIO	Central Imagery Office
CIO	Chief Information Officer
CIPA	Classified Information Procedures Act
CIRT	Computer Incident Response Team
CIS	Cryptologic Information System
CISARA	Counterintelligence, Security Countermeasures, and Related Activities
CISO	Counterintelligence Support Officer
CISP	Counterintelligence Support Plan
CISSM	Component Information System Security Manager
CISSP	Certified Information Systems Security Professional
CJCS	Chairman of the Joint Chiefs of Staff
CKTS	Computerized Key Telephone System
CLAS	Classified By
CLL	Chief of Legislative Liaison
CM	Chief of Mission
CM	Classification Management
CM	Configuration Management
CM	Countermeasure
CMB	Configuration Management Board
CMC	Command Master Chief (Navy)
CMC	Commandant of the Marine Corps

CMI	Classified Military Information
CMIWG	Classification Markings and Implementation Working Group
CMS	Community Management Staff
CMTS	Compliance, Monitoring and Tracking System
CMU	Concrete-Masonry Unit
CNA	Computer Network Attack
CNAC	National Agency Check plus Credit Check
CNACI	Child Care National Agency Check plus Written Inquires and Credit Check (OPM)
CNCI	Child Care National Agency Check plus Written Inquires and Credit Check
CNE	Computer Network Exploitation
CNO	Chief of Naval Operations
CNR	Chief of Naval Research
CNSI	Classified National Security Information
CNSS	Committee on National Security Systems
CNWDI	Critical Nuclear Weapon Design Information
CO	Commanding Officer
CO	Contracting Officer
CO	Cyberspace Operations
COCOM	Coordinating Committee
COD	Cooperative Opportunities Document
COI	Community Of Interest
COMINT	Communications Intelligence

COMPUSEC Computer Security
COMSEC Communications Security
CONEX Container Express
CONOPS Concept of Operations
CONPLAN Contingency Plan
CONUS Continental United States
COO Chief Operating Officer
COOP Continuity of Operations Plan
COP Common Operational Picture
C-OPE Cyber Operational Preparation of the Environment
COPS Committee on Physical Security
COR Central Office of Record
COR Contracting Officer Representative
COSMIC North Atlantic Treaty Organization (NATO) TOP SECRET
COTR Contracting Officer's Technical Representative
COTS Commercial Off-the-Shelf
COTS Committee on Technical Security
CP Command Post
CPAF Cost Plus Award Fee (Contract)
CPBX Computerized Private Branch Exchange
CPFF Cost Plus Fixed Fee (Contract)
CPI Critical Program Information
CPIF Cost Plus Incentive Fee (Contract)
CPM Command Program Manager
CPM Contractor Program Manager

CPO	Chemical Protection Over-Garment
CPP	Cooperative Program Personnel
CPP	Counter Proliferation Policy
C-PR	Confidential-Periodic Reinvestigation
CPSO	Command Program Security Officer
CPSO	Contractor Program Security Officer
CPU	Central Processing Unit
CPWG	Crime-Prevention Working Group
CQ	Charge of Quarters
CRG	Compliance Review Group
CRIMP	Crime Reduction Involving Many People
CRS	Congressional Research Service
CRT	Critical Research Technology
CRYPTO	Cryptography
CS&C	Office of Cybersecurity and Communications
CSA	Cognizant Security Agency
CSA	Cognizant Security Authority
CSA	Controlled Substances Act
CSBM	Confidence and Security Building Measure
CSC	Civil Service Commission
CSCS	Contract Security Classification Specification
CSE	Center for Security Evaluation
CSEA	Cyber Security Enhancement Act
CSIL	Critical and Sensitive Information List

CSISM	Communications Security (COMSEC) Supplement to the Industrial Security Manual
CSO	Cognizant Security Office
CSO	Court Security Officer
CSRA	Civil Service Reform Act
CSRL	Common Strategic Rotary Launcher
CSS	Central Security Service
CSS	Constant Surveillance Service
CSSI	Case Summary Sheet Information
CSSM	Communications-Computer System Security Manager
CSSO	Contractor Special Security Officer
CSSR	Case Summary Sheet Recommendation
CSSWG	Contractor SAP/SAR Security Working Group
CST	Construction Surveillance Technician
CT	Counter Terrorism
CT&E	Certification Test and Evaluation
CTA	Common Table of Allowance
CTB	Comprehensive Nuclear Test-Ban
CTBT	Comprehensive Nuclear Test-Ban Treaty
CTBTO	Comprehensive Nuclear Test-Ban Treaty Organization
CTC	Counterterrorist Center
CTF	Chemical Transfer Facility
CTR	Cooperative Threat Reduction Program
CTS	Computerized Telephone System

CTS	COSMIC TOP SECRET
CTSA	COSMIC TOP SECRET ATOMAL
CTTA	Certified Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Technical Authority
CUA	Co-Utilization Agreement
CUI	Controlled Unclassified Information
CUSR	Central United States Registry
CVA	Central Verification Activity
CVS	Contractor Verification System
CW	Chemical Warfare
CW	Chemical Weapons
CW	Code Word
CW	Cyber Warfare
CWC	Chemical Weapons Convention
CWCIP	Chemical Weapons Challenge Inspection Process
CWDF	Chemical Weapons Destruction Facility
CW-IWG	Chemical Weapons Implementation Working Group
CWPF	Chemical Weapons Production Facility
CWSF	Chemical Weapons Storage Facility

D

D.C.	District of Columbia
DA	Department of the Army
DAA	Designated Accrediting Authority
DAA	Designated Approving Authority

DAA Rep	Designated Accrediting/Approving/ Authority Representative
DAB	Defense Acquisition Board
DAC	Discretionary Access Control
DAE	Defense Acquisition Executive
DAF	Department of the Air Force
DAIG	Department of the Army Inspector General
DAO	Department/Agency/Organization
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DCAA	Defense Contract Audit Agency
DCAS	Defense Contract Administration Service
DCC	Defensive Counter-Cyber
DCFL	Defense Computer Forensics Lab
DCHC	Defense Counterintelligence and Human Intelligence Center
DCI	Director of Central Intelligence
DCI SSC	Director of Central Intelligence Special Security Center
DCID	Director of Central Intelligence Directive
DCII	Defense Central Index of Investigations
DCII	Defense Clearance and Investigations Index
DCIS	Defense Criminal Investigation Service
DCL	Declassify
DCMA	Defense Contract Management Agency

DCMC	Defense Contract Management Command
DCPDS	Defense Civilian Personnel Data System
DCPM	Defense Civilian Personnel Management
DCPMS	Defense Civilian Personnel Management System
DCR	Developed Character Reference
DCS	Defense Courier Service
DCS	Deputy Chief of Staff
DCS	Defense Clandestine Service
DCSINT	Deputy Chief of Staff for Intelligence, Army
DD	Defense Department
DDA	Designated Disclosure Authority
DDAL	Delegation of Disclosure Authority Letter
DDEP	Defense Data Exchange Program
DDL	Delegation of Disclosure Authority Letter
DDSP/G	Department of Defense Security Police/Guard
DEA	Drug Enforcement Administration
DECL	Declassify
DEERS	Defense Enrollment Eligibility Reporting System
DEIDS	Defense Eligibility Information Database System
DEPSECDEF	Deputy Secretary of Defense
DERV	Derived From
DES	Data Encryption Standard

DF	Declared Facility
DFA	Detailed/Draft Facility Agreement
DFAR	Defense Federal Acquisition Regulations
DFAS	Defense Finance and Accounting Service
DG	Director-General
DGR	Designated Government Representative
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIACAP	Department of Defense (DoD) Information Assurance Certification and Accreditation Process
DIAM	Defense Intelligence Agency Manual
DIC	Defense Intelligence Community
DICOB	Defense Industrial Security Clearance Oversight Board
DIDO	Designated Intelligence Disclosure Official
DII	Defense Information Infrastructure
DIRNSA	Director, National Security Agency
DIS	Defense Investigative Service
DISA	Defense Information Systems Agency
DISCO	Defense Industrial Security Clearance Office
DISCR	Directorate, Industrial Security Clearance Review
DISN	Defense Information Systems Network
DISP	Department of Defense (DoD) Industrial Security Program

DITSCAP	Department of Defense (DoD) Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DMDC	Defense Manpower Data Center
DMF	Data Management Facility
DMNS	Data Management Notification System
DMS	Data Management System
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DNA	Defense Nuclear Agency
DNG	Downgrade
DNI	Director of National Intelligence
DNI	Director of Naval Intelligence
DOB	Date of Birth
DOC	Department of Commerce
DoD	Department of Defense
DoD IG	Department of Defense Inspector General
DoDC	Department of Defense Component
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	Department of Defense Intelligence Information System
DoDIS	Department of Defense Information System
DoDM	Department of Defense Manual

DoDPI	Department of Defense Polygraph Institute
DoDSI	Department of Defense Security Institute
DOE	Department of Energy
DOHA	Defense Office of Hearings and Appeals
DOIS	Director of Industrial Security
DOJ	Department of Justice
DON	Department of the Navy
DONCAF	Department of the Navy Central Adjudication Facility
DOS	Denial of Service
DOS	Department of State
DOS	Disk Operating System
DOT	Department of Transportation
DPA	Defense Production Act
DPEP	Defense Personnel Exchange Program
DPG	Defense Planning Guidance
DPRB	Defense Planning and Resources Board
DPRO	Defense Plant Representative Office
DPS	Diplomatic Pouch Service
DRAM	Dynamic Random-Access Memory
DRB	Defense Resources Board
DRMO	Defense Reutilization Management Office
DS	Direct Support
DSA	Designated Security Authority
DSB	Defensive Security Brief
DSCA	Defense Security Cooperation Agency
DSEC	Director of Security

DSMC	Defense Systems Management College
DSN	Defense Switched Network
DSS	Defense Security Service
DSSCS	Defense Special Security Communication System
DSS-PIC	DSS Personnel Investigations Center
DSSS	Defense Special Security System
DT&E	Development Test and Evaluation
DTG	Date/Time Group
DTIC	Defense Technical Information Center
DTIRP	Defense Treaty Inspection Readiness Program
DTM	Data-Transmission Media
DTOC	Division Tactical Operations Center
DTRA	Defense Threat Reduction Agency
DTS	Defense Transportation Service
DTSA	Defense Technology Security Administration
DUSD SP	Deputy Under Secretary of Defense for Security Policy
DVD	Digital Video Disk

E

EA	Electronic Attack
EAA	Export Administration Act
EABX	Electronic Private Automatic Branch Exchange

EAP Emergency Action Plan
EARS Export Administration Regulations
EC Executive Council
ECCM Electronic Counter-Countermeasures
ECINT Economic Intelligence
ECM Electronic Countermeasures
EDM Emergency-Destruct Measures
EECS Electronic Entry-Control System
EEFI Essential Elements of Friendly Information
EEI Essential Elements of Information
EEOC Equal Employment Opportunity Commission
EEPROM Electronically Erasable Programmable Read-Only Memory
EI Essential Elements of Information
EIF Entry/Entered-Into-Force
EIS-TAO Enterprise Information Systems-Technology Applications Office
EKMS Electronic Key Management System
EL Export License
ELA Export License Application
ELECTRO-OPTINT Electrical Optical Intelligence
ELINT Electronic Intelligence
ELSEC Electronic Security
EMSEC Emanation Security
EMSEC Emission Security
ENAC Entrance National Agency Check
ENAL Entrance National Agency Check

	plus Special Investigative Inquiry
ENTNAC	Entrance National Agency Check
EO	Executive Order
EOC	Emergency Operations Center
EOD	Explosive-Ordnance Disposal
EOR	Element of Resource
EP	Electronic Protection
EPA	Environmental Protection Agency
EPCI	Enhanced Proliferation Control Initiative
EPITS	Essential Program Information, Technologies and Systems
EPL	Evaluated Products List
EPROM	Erasable Programmable Read-Only Memory
EPSQ	Electronic Personnel Security Questionnaire
EPW	Enemy Prisoner of War
e-QIP	Electronic Questionnaire for Investigative Processing
ERB	Engineering Review Board
ES	Electronic Surveillance
ES	Executive Secretary
ESEP	Engineer and Scientist Exchange Program
ESM	Extraordinary Security Measure
ESS	Electronic Security System
ET	Electronic Transmission
ET	Escort Team
ETZ	Equipment Transient Electromagnetic

	Pulse Emanation Standard (TEMPEST) Zone
EU	European Union
EW	Electronic Warfare
EWS	Electronic Warfare Support

F

FA	Facility Agreement
FAA	Federal Aviation Administration
FAA	Foreign Assistance Act
FAD	Facility Access Determination
FAR	Federal Acquisition Regulation
FAX	Facsimile
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FCB	File Control Block
FCC	Federal Communications Commission
FCG	Foreign Clearance Guide
FCIP	Foreign Counterintelligence Program
FCL	Facility Security Clearance
FCT	Foreign Comparative Test
FD	Foreign Disclosure
FD POC	Foreign Disclosure Point of Contact
FDO	Foreign Disclosure Officer
FDS	Facility Data Sheet
FEMA	Federal Emergency Management Agency
FEPROM	Flash Erasable Programmable Read-Only Memory

FFC	Fixed Facility Checklist
FFP	Firm Fixed Price (Contract)
FFRDC	Federally Funded Research and Development Center
FGI	Foreign Government Information
FHB	Former Heavy Bomber
FI	Foreign Intelligence
FIDS	Facility Intrusion Detection System
FIE	Foreign Intelligence Entity
FIEPSS	Fixed Installation Exterior Perimeter Security System
FINCEN	Financial Crimes Enforcement Network
FIPC	Federal Investigations Processing Center
FIS	Foreign Intelligence Services
FISA	Foreign Intelligence Surveillance Act
FISD	Federal Investigative Services Division
FISINT	Foreign Instrumentation Signals Intelligence
FISMA	Federal Information Security Management Act
FIT	Foreign Inspection Team
FIU	Field Investigative Unit
FLO	Foreign Liaison Officer
FLRA	Federal Labor Relations Authority
FM	Frequency-Modulated
FMCT	Fissile Material Cutoff Treaty
FMS	Foreign Military Sales
FN	Foreign National

FOA	Field Operating Agency
FOC	Full Operational Capability
FOCI	Foreign Ownership, Control or Influence
FOIA	Freedom of Information Act
FOIA/PA	Freedom of Information Act/Privacy Act
FORDTIS	Foreign Disclosure and Technical Information System
FOUO	For Official Use Only
FPI	Fixed Price Incentive (Contract)
FPIF	Fixed Price Incentive Firm (Contract)
FPM	Federal Personnel Manual
FRAM	Ferroelectric Random-Access Memory
FRD	Formerly Restricted Data
FRS	Facility Review Subgroup
FSC	Forum for Security Cooperation
FSL	Fixed Structure for Launcher
FSO	Facility Security Officer
FSP	Facility Security Profile
FSS	Federal Supply Schedule
FSTS	Federal Security Telephone Service
FSU	Former Soviet Union
FTZ	Facilities Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Zone
FVS	Foreign Visits System
FWA	Fraud, Waste, and Abuse
FY	Fiscal Year
FYDP	Five Year Defense Plan

G

G	GAMMA
G&A	General and Administrative
G2	Assistant Chief of Staff, G2 Intelligence
G-2	Staff Intelligence Officer
GAO	General Accounting Office
GC/MS	Gas Chromatography/Mass Spectrometry
GCA	Government Contracting Activity
GCCS	Global Command and Control System
GCO	GAMMA Control Officer
GDIP	General Defense Intelligence Programs
GENSER	General Service
GEOINT	Geospatial Intelligence
GFE	Government Furnished Equipment
GFP	Government Furnished/Furnished Property
GHz	Gigahertz
GIG	Global Information Grid
GII	Global Information Infrastructure
GLBM	Ground-Launched Ballistic Missile
GLCM	Ground-Launched Cruise Missile
GMT	Greenwich Mean Time
GOCO	Government-Owned, Contractor-Operated
GOTS	Government Off-The-Shelf
GOVIND	Government-Industry Restricted Information
GPM	Government Program Manager

GPS	Global Positioning System
GSA	General Security Agreement
GSA	General Services Administration
GSA	Government Services Administration
GSC	Government Security Committee
GSOIA	General Security of Information Agreement
GSOMIA	General Security of Military Information Agreement
GTA	Graphic Training Aid

H

HAC	House Appropriations Committee
HAS	Hardened Aircraft Shelter
HASC	House Armed Services Committee
HB	Heavy Bomber
HCA	Host Country Agreement
HDBT	Hardened and Deeply Buried Target
HDMI	High-Definition Multimedia Interface
HE	High Explosive
HEU	Highly Enriched Uranium
HN	Host Nation
HNSC	House National Security Committee
HOF	Home Office Facility
HOIS	Hostile Intelligence Services
HPSCI	House Permanent Select Committee on Intelligence

HQ Headquarters
HQ AFOTEC Headquarters, Air Force Operational Test and Evaluation Center
HQ USAF/XOF Headquarters, Air Force Security Forces
HRO Human Resources Office
HSA Homeland Security Act
HSP Host State Party
HSPD Homeland Security Presidential Directive
HT Host Team
HTL Host Team Leader
HUMINT Human Intelligence
HVAC Heating, Ventilation and Air Conditioning
HVSACO Handle Via Special Access Channels Only
Hz Hertz

I

IA Information Assurance
IA Intelligence Activity
IAA Interim Access Authorization
IACSE Interagency Advisory Committee on Security Equipment
IAEA International Atomic Energy Agency
IAM Information Assurance Manager
IAO Information Assurance Officer
IAO Interim Approval to Operate
IAR Information Assurance Representative
IAT Installation Assistance Team
IATO Interim Approval To Operate

IATT	Interim Approval To Test
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IBI	Interview Oriented Background Investigation
IC	Intelligence Community
ICAM	Improved Chemical Agent Monitor
ICAO	International Civil Aviation Organization
ICBM	Intercontinental Ballistic Missile
ICC	Inspection Coordination Center
ICC	Interstate Commerce Commission
ICD	Initial Capabilities Document
ICD	Intelligence Community Directive
ICP	Initial Control Point
ICR	Inventory Change Report
ID	Identification
IDC	International Data Center
IDE	Intrusion Detection Equipment
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IEID	International Exchange of Infrasound Data
IERD	International Exchange of Radionuclide Data
IESD	International Exchange of Seismological Data
IG	Inspector General

IG DoD	Inspector General of the Department of Defense
IID	Improvised Incendiary Device
IIR	Intelligence Information Report
IIT	International Inspection Team
IIV	Interim Inventory Verification
IMA	Intelligence Materiel Activity
IMD	Intelligence Material Detachment
IMINT	Imagery Intelligence
IMS	International Monitoring System
IMSP	Information Management Support Plan
INA	Integrated Notifications Application
INF	Intermediate-Range Nuclear Forces Treaty
INFCIRC	Information Circular
INFOSEC	Information Systems Security
INFOWAR	Information Warfare
INMARSAT	International Maritime Satellite
IN-SAP	Intelligence Special Access Program
INSCOM	United States (U.S.) Army Intelligence and Security Command
INTAC	Individual Terrorism Awareness Course
INTCOL	Intelligence Collection
Interior	Department of the Interior
IOC	Initial Operating Capability
IOC	Intelligence Operations Center
IOI	Item of Inspection

IOSS	Interagency Operations Security (OPSEC) Support Staff
IOT&E	Initial Operational Test and Evaluation
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlefield
IPDS	Improved Point Detection System (Chemical Agent)
IPE	Individual Protection Equipment
IPIV	Initial Physical Inventory Verification
IPO	International Pact Organization
IPO	International Program Office
IPSAC	Interagency Security Classification Appeals Panel
IR	Infrared
IR&D	Independent Research and Development
IRAC	Internal Review and Audit Compliance
IRBM	Intermediate-Range Ballistic Missile
IRCA	Immigration Reform and Control Act
IRM	Information Resource Management
IRP	Inspection Readiness Plan
IS	Information System
IS	Inspectable Space
ISA	International Security Agreement
ISB	Industrial Security Bulletin
ISCAP	Interagency Security Classification Appeals Panel
ISCOM	Naval Investigative Service Command
ISD	Information Storage Device

ISD	Inspectable Space Determination
ISDN	Integrated Services Digital Network
ISFD	Industrial Security Facilities Database
ISL	Industrial Security Letter
ISM	Industrial Security Manual
ISOO	Information Security Oversight Office
ISP	Inspected State Party
ISPG	Intelligence Programs Support Group
ISR	Industrial Security Regulation
ISRP	Information Systems Requirements Package
ISS	Information Systems Security
ISS	Inspection Support Staff
ISS	Integrated Safeguards Subgroup
ISSE	Information System Security Engineer
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Professional
ISSR	Information Systems Security Representative
ISWG	Industrial Security Working Group
IT	Information Technology
IT	Inspection Team
ITAB	Information Technology Acquisition Board
ITAC	Intelligence and Threat Analysis Center
ITAR	International Traffic in Arms Regulations
ITC	Interagency Training Center
IVP	International Visit Program

IWC	Inhumane Weapons Convention
IWG	Interagency Working Group

J

J2	Intelligence Directorate, Joint Command
JACADS	Johnston Atoll Chemical Agent Disposal System
JACIG	Joint Arms Control Implementation Group
JAFAN	Joint Air Force-Army-Navy
JAG	Judge Advocate General
JAGMAN	Judge Advocate General Manual
JAMS	Joint Adjudications Management System
JANAP	Joint Army, Navy, Air Force Publication
JCAVS	Joint Clearance and Access Verification System
JCG	Joint Consultative Group
JCIC	Joint Compliance and Inspection Commission
JCITA	Joint Counterintelligence Training Academy
JCS	Joint Chiefs of Staff
JMIC	Joint Military Intelligence College
JMIP	Joint Military Intelligence Programs
JMITC	Joint Military Intelligence Training Center
JPAS	Joint Personnel Adjudication System
JROC	Joint Requirements Oversight Council
JS	Joint Service

JS	Joint Staff
JSAIWG	Joint Sensitive Compartmented Information (SCI) Accreditation/ Inspection Working Group
JSAT	Joint Security Assistance Training
JSCP	Joint Strategic Capabilities Plan
J-SIIDS	Joint Services Interior Intrusion Detection System
JSP	Joint Service Program
JTF	Joint Trial Flight
J-TIDS	Joint Tactical Information Distribution System
JUA	Joint Use Agreement
JVE	Joint Verification Experiment
JWICS	Joint Worldwide Intelligence Communication System
kHz	Kilohertz

K

KMID	Key Material Identification Number
KMP	Key Management Personnel
KSU	Key Service Unit
KT	Kiloton

L

LAA	Limited Access Authorization
LAC	Local Agency Check

LAN	Local Area Network
LBI	Limited Background Investigation
LBIP	Limited Background Investigation plus Current National Agency Check
LBIX	Limited Background Investigation Expanded
LBNA	Land-Based Naval Air
LC	Launch Canister
LCA	Limited Controlled Area
LCR	Listed Character Reference
LE	Law Enforcement
LEA	Law Enforcement Agency
LED	Light-Emitting Diode
LEU	Low Enriched Uranium
LFC	Local Files Check
LIMDIS	Limited Dissemination
LIMDIS	Limited Distribution
LLC	Limited Liability Corporation
LN	Local Network
LOA	Letter of Agreement
LOA	Letter of Offer and Acceptance
LOC	Letter of Consent
LOC	Level of Concern
LOD	Letter of Denial
LOI	Letter of Intent
LON	Letter of Notification
LOS	Line of Sight
LOTS	Logistics Over The Shore

LP	Listening Post
LPD	Low Probability of Detection
LPF	Launcher Production Facility
LPI	Low Probability of Intercept
LRA	Local Reproduction Authorized
LRC	Local Records Check
LRCN	Local Records Checks plus Investigation Requested
LRF	Launcher Repair Facility
LRIP	Low Rate Initial Production
LRNA	Long-Range Nuclear Air- Launched [Cruise Missile]
LRU	Lowest Replaceable Unit
LSF	Launcher Storage Facility
LSN	Local Seismic Network
LTBT	Limited Test-Ban Treaty
LTM	Long-Term Monitoring

M

MA	Milliamperes
MAA	Mission Area Analysis
MAC	Mandatory Access Control
MAC	Military Airlift Command
MACOM	Major Command
MAD	Mutual Assured Destruction
MAIS	Major Automated Information Systems
MAJCOM	Major Joint Command

MANPAD	Man-Portable Air Defense System
MASINT	Measurement and Signature Intelligence
MBA	Material Balance Area
MBF	Military Biological Facility
MBI	Minimum Background Investigation
MBIP	Minimum Background Investigation plus Current National Agency Check
MBIX	Minimum Background Investigation Expanded
MBR	Material Balance Report
MBT	Main Battle Tank
MC	Mitigating Conditions
MC&A	Materials Control and Accounting/ Accountability
MCL	Munitions Control List
MCO	Marine Corps Order
MCT	Militarily Critical Technology
MCTL	Militarily Critical Technologies List
MDA	Milestone Decision Authorities
MDA	Missile Defense Agency
MDAP	Major Defense Acquisition Program
MDEP	Management Decision Package
MDMP	Military Decision-Making Process
MEVA	Mission-Essential or Vulnerable Area
MF	Maintenance Facility
MFA	Model Facility Agreement
MFO	Multiple Facility Organization
MI	Military Intelligence

MILCON	Military Construction
MILDEP	Military Department
MIL-STD	Military Standard
MINATOM	Ministry of Atomic Energy (Russian Federation)
MIRV	Multiple Independently- Targetable Reentry Vehicle
MISWG	Multinational Industrial Security Working Group
MLRS	Multiple Launch Rocket System
MNS	Mission Need Statement
MO	Magneto-Optical
MO	Modus Operandi
MOA	Memorandum of Agreement
MOBDES	Mobilization Designee
MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
MP	Military Police/Manipulation Proof
MPACS	Military Police Automated Control System
MR	Mandatory Review
MRBM	Medium-Range Ballistic Missile
MRI	Mutual Reciprocal Inspection
MRV	Multiple Reentry Vehicle
MSDDC	Military Surface Deployment and Distribution Command
MS-DOS	Microsoft Disk Operating System
MSIC	Military and Space Intelligence Center
MSPB	Merit Systems Protection Board

MSS	Munitions Sampling System
MT	Megaton
MTCR	Missile Technology Control Regime
MTMC	Military Traffic Management Command
MUF	Material Unaccounted For
MWD	Military Working Dog

N

NA	National Authority
NAC	National Agency Check
NACB	National Agency Check plus Written Inquiries and Credit Check plus Background Investigation Requested
NACI	National Agency Check plus Written Inquiries
NACIC	National Counterintelligence Center
NACL	National Agency Check plus Special Investigative Inquiry
NACLC	National Agency Check with Local Agency Checks and Credit Check
NACP	National Agency Check plus 10 Years of Service
NACS	National Authority Coordinating Staff
NACSIM	National COMSEC Information Memorandum
NACW	National Agency Check plus Written Inquiries and Credit Check

NACZ	National Agency Check plus Written Inquiries and Credit Check plus Special Investigative Inquiry
NAF	Naval Air Facility
NAF	Non-Appropriated Funds
NAFI	Non-Appropriated Fund Investigation
NAG/SCM	National Advisory Group/Security Countermeasures
NAIC	National Air Intelligence Center
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAVATAC	Navy Antiterrorism Analysis Center
NAVCIRT	Navy Computer Incident Response Team
NAVIPO	Navy International Programs Office
NBC	Nuclear, Biological, and Chemical
NC	No Contract
NC	North Atlantic Treaty Organization (NATO) CONFIDENTIAL
NCA	National Command Authority
NCA	North Atlantic Treaty Organization (NATO) CONFIDENTIAL ATOMAL
NCAF	Department of Navy Central Adjudication Facility
NCAS	National Cyber Alert System

NCCIC	National Cybersecurity and Communications Integration Center
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NCMS	National Classification Management Society
NCO	Non-Commissioned Officer
NCRAL	National Cyber Risk Alert Level
NCS	National Communications System
NCS	National Cryptologic School
NCSC	National Computer Security Center
NCSD	National Cyber Security Division
NDA	Non-Destructive Assay
NDA	Non-Disclosure Agreement
NDE	Non-Destructive Evaluation
NDP	National Disclosure Policy
NDP-1	National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations
NDPC	National Disclosure Policy Committee
NDS	Non-Disclosure Statement
Net	Network
NETMGR	Network Manager
NetOps	Network Operations
NF	Not Releasable to Foreign Nationals
NFIB	National Foreign Intelligence Board
NFIP	National Foreign Intelligence Program

NFX	Nuclear-Free Zone
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NGO	Non-Governmental Organization
NIAG	North Atlantic Treaty Organization (NATO) Industrial Advisory Group
NIAP	National Information Assurance Partnership
NID	National Interest Determination
NII	National Information Infrastructure
NIMA	National Imagery and Mapping Agency
NIPRNET	Non-Secure/Unclassified Internet Protocol Router Network
NIS	Naval Investigative Service
NIS	Network Information System
NISC	Naval Investigative Service Command
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISPOMSUP	National Industrial Security Program Operating Manual Supplement
NISPPAC	National Industrial Security Program Policy Advisory Committee
NIST	National Institute of Standards and Technology
NLC	National Agency Check plus Local Agency Check plus Credit Check

NLT	Not Later Than
NMD	National Missile Defense
NMI	No Middle Initial
NMMSS	Nuclear Materials Management Safeguards System
NMN	No Middle Name
NMS-CO	National Military Strategy for Cyberspace Operations
NN	Nickname
NNAC	National Agency Check plus Written Inquiries and Credit Check plus Current National Agency Check
NNAG	North Atlantic Treaty Organization (NATO) Naval Armaments Group
NNPA	Nuclear Non-Proliferation Act
NNPI	Naval Nuclear Propulsion Information
NNWS	Non-Nuclear Weapon State
NOAC	National Operational Security Advisory Committee
NOFORN	Not Releasable to Foreign Nationals
NPC	Nonproliferation Center
NPI	No Pertinent Information
NPLO	North Atlantic Treaty Organization (NATO) Production and Logistics Organization
NPRC	National Personnel Records Center
NPRDC	Naval Personnel Research and Development Center

NPSB	National Agency Check plus Partial Special Background Investigation
NPT	Nuclear Non-Proliferation Treaty
NR	North Atlantic Treaty Organization (NATO) Restricted
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NRRC	Nuclear Risk Reduction Center
NS	North Atlantic Treaty Organization (NATO) SECRET
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSA	North Atlantic Treaty Organization (NATO) SECRET ATOMAL
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NSCO	North Atlantic Treaty Organization (NATO) SECRET Control Officer
NSD	National Security Directive
NSDD	National Security Decision Directive
NSDM	National Security Decision Memorandum
NSF	National Science Foundation
NSG	Nuclear Suppliers Group
NSI	National Security Information
NS-IWG	Nuclear Safeguards Implementation Working Group

NSM	Network Security Manager
NSN	National Stock Number
NSO	Network Security Officer
NSS	National Security System
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
NSTISSC	National Security Telecommunication Information Systems Security Committee
NSTISSI	National Security Telecommunications Information Systems Security Instruction
NSTL	National Security Threat List
NTI	National Trial Inspection
NTISSC	National Telecommunications and Information Systems Security Commission
NTISSI	National Telecommunications and Information Systems Security Instruction
NTISSP	National Telecommunications and Information Systems Security Policy
NTK	Need-To-Know
NTM	National Technical Means
NTS	Nevada Test Site
NTT	Nuclear Testing Treaties
NU	North Atlantic Treaty Organization (NATO) UNCLASSIFIED
NVD	Night-Vision Device
NVM	Non-Volatile Memory
NVRAM	Non-Volatile Random-Access Memory

NWFZ	Nuclear-Weapon Free Zone
NWS	Nuclear-Weapon State
NWSS	Nuclear Weapon Storage Site

O

O&S	Operations and Support
OA, EOP	Office of Administration, Executive Office of the President
OADR	Originating Agency Determination Required
OASD	Office of the Assistant Secretary of Defense
OCA	Original Classification Authority
OCO	Offensive Cyberspace Operations
OCONUS	Outside the Continental United States
ODC	Office of Defense Cooperation
ODCI	Office of the Director of Central Intelligence
ODNI	Office of the Director of National Intelligence
ODTC	Office of Defense Trade Controls
Oe	Oersted
OI	Operating Instruction
OIAR	Office of Information and Regulatory Affairs
OIG	Office of the Inspector General
OIS	Office Information System
OISI	Office of Industrial Security, International

OJCS	Organization of the Joint Chiefs of Staff
OMB	Office of Management and Budget
OMIM	Operational Manual for Infrasound Monitoring
OMOSI	Operational Manual for On-Site Inspections
OMRM	Operational Manual for Radionuclide Monitoring
OMSM	Operational Manual for Seismological Monitoring
ONDCP	Office of National Drug Control Policy
ONI	Office of Naval Intelligence
OODEP	Owners, Officers, Directors, Executive Personnel
OOV	Object of Verification
OPAC-ALC	On-line Payment and Collection-Agency Locator Code
OPCW	Organization for the Prohibition of Chemical Weapons
OPF	Official Personnel File
OPIC	Overseas Private Investment Corporation
OPLAN	Operations Plan
OPM	Office of Personnel Management
OPORD	Operations Order
OPR	Office of Primary Responsibility
OPSEC	Operations Security
ORCON	Dissemination and Extraction of Information Controlled by Originator

ORD	Operational Requirements Document
OS	Operating System
OS	Treaty on Open Skies
OSC	Office of Special Counsel
OSCC	Open Skies Consultative Commission
OSCE	Organization for Security and Cooperation in Europe
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
OSI	On-Site Inspection
OSINT	Open Source Intelligence
OSMAPS	Open Skies Management and Planning System
OSP	Operations Security Plan
OSPB	Overseas Security Policy Board
OSPG	Overseas Security Policy Group
OSRA	Open Skies Refueling Aircraft
OS-SAP	Operations and Support Special Access Program
OSTP	Office of Science and Technology Policy
OT&E	Operational Test and Evaluation
OTA	Office of Technical Assessment
OUSD A&T	Office of the Under Secretary of Defense, Acquisition and Technology
OVP	Office of the Vice President
OWG	Operations Security Working Group

P

PA	Privacy Act
PAA	Principal Accrediting Authority
PAA	Principal Approving Authority
PABX	Private Automatic Branch Exchange
PAC	Personnel Access Ceiling
PAL	Permissive Action Link
PAR	Program Access Request
PAS	Protected Aircraft Shelter
PASCODE	Personnel Accounting System Code
PB	President's Budget
PBD	Program Budget Decision
PBX	Private Branch Exchange
PC	Peace Corps
PC	Personal Computer
PCD	Portable Computing Device
PCL	Personnel Security Clearance
PCO	Procuring Contracting Officer
PCS	Permanent Change of Station
PCU	Premise Control Unit
PD	Probability of Detection
PD	Public Domain
PDA	Personal Digital Assistant
PDA	Principal Disclosure Authority
PDD	Personal Digital Diary
PDD	Presidential Decision Directive
PDM	Program Decision Memorandum

PDR	Preliminary Design Review
PDS	Practice Dangerous to Security
PDS	Protected Distribution System
PDS	Public Domain Software
PED	Portable Electronic Device
PEM	Program Element Monitor
PEO	Program Executive Office
PEO-EIS	Program Executive Office, Enterprise Information Systems
PEP	Personnel Exchange Program
PERSEC	Personnel Security
PERSEREC	Personnel Security Research and Evaluation Center
PFIAB	President's Foreign Intelligence Advisory Board
PFS	Personal Financial Statement
PHOTINT	Photographic Intelligence
PHYSEC	Physical Security
PI	Police Intelligence
PI	Preliminary Inquiry
PID	Personnel Identification Data
PII	Personally Identifiable Information
PIL	Physical Inventory Listing
PINS	Portable Isotope Neutron Spectroscopy
PIPS	Personnel Investigations Processing System
PIR	Passive Infrared
PIV	Physical Inventory Verification

PKI	Public Key Infrastructure
PL	Protection Level
PL	Public Law
PLA	Plain Language Address
PLAN	Operation Plan
PM	Program Manager
PM	Project Manager
PMCSD	Project Manager for Chemical Stockpile Disposal
PMD	Program Management Directive
PMNSCM	Program Manager for Non-Stockpile Chemical Material
PMO	Program Management Office
PMO	Provost Marshal Office
PNE	Peaceful Nuclear Explosion
PNET	Peaceful Nuclear Explosions Treaty
PO	Program Office
POB	Place of Birth
POC	Point of Contact
POE	Point of Entry/Exit
POL	Petroleum, Oil, and Lubricants
POM	Program Objective Memorandum
PONEI	Protocol on Notifications and Exchange of Information
POV	Privately Owned Vehicle
PPBERS	Planning, Programming, and Budgeting Execution Review System

PPBS	Planning, Programming, and Budgeting System
PPCM	Perimeter and Portal Continuous Monitoring
PPP	Program Protection Plan
PPPF	Permitted Schedule 1 Protective Purposes Facility
PPR	Phased Periodic Reinvestigation
PPRA	Plutonium Production Reactor Agreement
PR	Periodic Reinvestigation
PREPCOM	Preparatory Commission/ Committee
PREPCON	Preparatory Conference
PRI	Periodic Reinvestigation
PROM	Programmable Read-Only Memory
PROPIN	Proprietary Information
PRP	Personnel Reliability Program
PRS	Periodic Reinvestigation-SECRET
PRSC	Periodic Reinvestigation-SECRET/ CONFIDENTIAL
PS	Physical Security
PSAB	Personnel Security Appeals Board
PSAP	Prospective Special Access Program
PSD	Program Security Directive
PSD	Protective Security Detail
PSE	Physical Security Equipment
PSEAG	Physical Security Equipment Action Group
PSF	Phosphorus, Sulfur, or Fluorine Discreet Organic Chemicals

PSG	Program Security Guide
PSI	Personnel Security Investigation
PSI	Physical Security Inspector
PSI	Program Security Instruction
PSI	Proliferation Security Initiative
PSM	Program Security Manager
PSO	Program Security Officer
PSP	Personnel Security Program
PSQ	Personnel Security Questionnaire
PSS	Personnel Security Specialist
PSS	Protective Security Service
PSWG	Personnel Security Working Group
PSYOP	Psychological Operations
PTBT	Partial Test-Ban Treaty
PU	Plutonium

Q

QA	Quality Assurance
QC	Quality Control
QNSP	Questionnaire for National Security Positions

R

R&D	Research and Development
RA	Restricted Area
RAC	Request Authority to Conclude an Agreement

RAISE	Rapid Assessment Incomplete Security Evaluation
RAM	Random-Access Memory
RAN	Request Authority to Negotiate an Agreement
RBAC	Role-Based Access Control
RCA	Riot Control Agent
RD	Restricted Data
RD&E	Research, Development, and Engineering
RDA	Research, Development, and Acquisition
RDE	Radiation Detection Equipment
RDT&E	Research, Development, Test, and Evaluation
REL TO	Releasable To
REMBASS	Remotely Monitored Battlefield Sensor System
REVCON	Review Conference
RF	Radio Frequency
RFA	Report for Adjudication
RFI	Radio Frequency Interference
RFI	Representative of a Foreign Interest
RFID	Radio-Frequency Identification
RFP	Request for Proposal
RFQ	Request for Quotation
RI	Report of Investigation
RII	Relevant Information and Intelligence
RIS	Reporting Identification Symbol
RL	Rocket Launcher

RLVP	Residual Level Validation Period
RM	Risk Management
RNLTD	Report Not Later Than Date
ROI	Report of Investigation
ROM	Read-Only Memory
RON	Report of National Agency Check
ROTC	Reserve Officer Training Corps
RPO	Responsible Program/Project Office
RRU	Research, Recertify, Upgrade
RSI	Reimbursable Suitability Investigation
RSN	Reason for Classification (Electronic Messages)
RSO	Requesting State Party Observer
RTP	Research and Technology Protection
RTSO	Remote Terminal Security Officer
RUC	Reporting Unit Code
RV	Reentry Vehicle
RVOSI	Reentry Vehicle On-Site Inspection

S

S	SECRET
S&T	Science and Technology
S2	Intelligence Officer, U.S. Army
SA	System Administrator
SA/LW	Small Arms/Light Weapons
SAA	Special Approval Authority
SAC	Senate Appropriations Committee

SACS	Security Access Control Systems
SAES	Security Awareness and Education Sub-committee
SAEWG	Security Awareness and Education Working Group
SAF	Secretary of the Air Force
SALT	Strategic Arms Limitation Talks
SAM	Surface-to-Air Missile
SAMM	Security Assistance Management Manual
SAO	Senior Agency Official
SAO	Special Access Office
SAP	Special Access Program
SAPCAF	Special Access Program Central Adjudication Facility
SAPCO	Special Access Program Central Office (Component)
SAPCO	Special Access Program Control Officer
SAPCO	Special Access Program Coordination Office (OSD)
SAPF	Special Access Program Facility
SAPI	Special Access Program Information
SAPOC	Special Access Program Oversight Committee
SAPWG	Special Access Program Working Group
SAR	Special Access Required
SAR	Synthetic Aperture Radar
SASC	Senate Armed Services Committee
SAT	Site Assistance/Assessment Team

SAV	Site Assistance/Assessment Visit or Visit with Special Right of Access
SBA	Small Business Administration
SBI	Special Background Investigation
SBII	Special Background Investigation plus Current National Agency Check
SBIP	Special Background Investigation/ Single Scope Background Investigation plus Current National Agency Check
SBIR	Single Scope Background Investigation Requested
SBPR	Periodic Reinvestigation of Special Background Investigation/Single Scope Background Investigation
SCA	Security Control Agreement
SAR	Special Access Required
SCBA	Self-Contained Breathing Apparatus
SCC	Standing Consultative Commission
SCE	Service Cryptologic Element
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCIPCCOM	Sensitive Compartmented Information Policy Coordination Committee
SCM	Security Countermeasure
SCR	Suspicious Contact Report
SD	Security Director

SDD	Secure Data Device
SDD	System Development and Demonstration
SDDC	Surface Deployment and Distribution Command
SDI	Strategic Defense Initiative
SDIO	Strategic Defense Initiative Organization
SDR	System Design Review
SDSO	System Design Security Officer
SEC	Securities and Exchange Commission
SECAF	Secretary of the Air Force
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SECNAV INST	Secretary of the Navy Instruction
SES	Senior Executive Service
SETA	Security Education, Training and Awareness
SETL	Security Environment Threat List
SF	Security Forces
SF	Special Forces
SF	Standard Form
SFO	Senior Foreign Official
SI	Special Intelligence
SICBM	Small Intercontinental Ballistic Missile
SID	Security-In-Depth
SIF	Special/Suitability Issue File
SIGINT	Signals Intelligence
SIGSEC	Signals Security
SII	Special Investigative Inquiry

SII	Suitability/Security Investigation Index
SIO	Senior Intelligence Officer
SIOP	Single Integrated Operations Plan
SIOP/ESI	Single Integrated Operational Plan/ Extremely Sensitive Information
SIPRNET	SECRET Internet Protocol Router/ Routing Network
SIR	Safeguards Implementation Report
SIRT	Security Incident Response Team
SISR	Signals Intelligence Security Regulation
SJA	Staff Judge Advocate
SLBM	Sea-Launched/Submarine-Launched Ballistic Missile
SLCM	Sea-Launched Cruise Missile
SLV	Space Launch Vehicle
SM	Security Manager
SME	Significant Military Equipment
SME	Subject Matter Expert
SMO	Security Management Office
SNDV	Strategic Nuclear Delivery Vehicle
SNM	Special Nuclear Material
SO/LIC	Special Operations/Low-Intensity Conflict
SOF	Special Operations Forces
SOFA	Status of Forces Agreement
SOFAR	Sound Fixing and Ranging
SOI	Security Officer Identifier
SOIC	Senior Official of the Intelligence Community

SON	Statement of Need
SON	Submitting Office Number
SOP	Standard Operating Procedures
SOR	Statement of Reasons
SOR	Statement of Requirement
SORT	Strategic Offensive Reductions Treaty
SOW	Statement of Work
SP	Security Police
SP	State Party
SPA	Special Purpose Access
SPAN	Security Policy Automation Network
SPB	Security Policy Board
SPECAT	Special Category
SPF	Security Policy Forum
SPG	Security Procedures Guide
SPINTCOM	Special Intelligence Communications
SPO	System Program Office
SPOC	Special Access Required (SAR) Programs Oversight Committee
SPP	Standard Practice Procedures
SPR	SECRET-Periodic Reinvestigation
SPRG	Special Programs Review Group
SPSCI	Senate Permanent Select Committee on Intelligence
SPSCIF	Semi-Permanent Sensitive Compartmented
SPT	Site Preparation Team
SRAM	Static Random-Access Memory

SRBM	Short-Range Ballistic Missile
SRF	Strategic Rocket Forces
SRG	Senior Review Group
SRM	Solid Rocket Motor
SRO	Special Review Office
SRR	System Requirements Review
SRTM	Security Requirements Traceability Matrix
SSA	Secure Storage Area
SSA	Special Security Agreement
SSAA	System Security Authorization Agreement
SSAN	Social Security Account Number
SSBI	Single Scope Background Investigation
SSBI-PR	Single Scope Background Investigation-Periodic Reinvestigation
SSBN	Nuclear-Powered Ballistic Missile
SSC	Special Security Center
SSCI	Senate Select Committee on Intelligence
SSCO	Special Security Contract Officer
SSDC	Space and Strategic Defense Command
SSE	System Security Engineering
SSEM	System Security Engineering Manager/Management
SSI	Suspect-Site Inspection
SSII	Suitability/Security Investigations Index
SSM	Site Security Manager
SSM	Surface-to-Surface Missile
SSM	System Security Manager
SSMP	System Security Management Plan

SSN	Social Security Number
SSO	Special Security Officer
SSP	System Security Plan
SSR	Special Security Representative
SSS	Security Support Structure
SSS	Selective Service System
SSS	Signature Security Service
SSS	Strengthened Safeguards System
SSSF	Single Small-Scale Facility
SSSP	Site Safeguards and Security Plan
SST	Site Survey Team
ST&E	Security Test and Evaluation
STA	System Threat Assessment
STANO	Surveillance, Target Acquisition, and Night Observation
STAR	System Threat Assessment Report
START	Strategic Arms Reduction Treaty
STC	Sound-Transmission Coefficient
STD	Standard
STE	Secure Telephone Equipment
STI	Safeguards, Transparency, and Irreversibility
STS	Safeguards Technology Subgroup
STU	Secure Telephone Unit
SVC	Special Verification Commission

T

T&E	Test and Evaluation

TA/CP	Technology Assessment and Control Plan
TAD	Temporary Duty Assignment
TAFMSD	Total Active Federal Military Service Date
TAO	Technology Applications Office
TASM	Tactical Air-to-Surface Missile
TASO	Terminal Area Security Officer
T-ATO	Tactical Approval to Operate
TB	Technical Bulletin
TBD	To Be Determined
TC	Team Chief
TCB	Trusted Computing Base
TCO	Technology Control Officer
TCO	Termination Contracting Officer
TCO	Treaty Compliance Officer
TCP	Technology Control Plan
TCS	Temporary Change of Station
TCS	Trusted Computer System
TDP	Technical Data Package
TDS	Technical Development Strategy
TDY	Temporary Duty
TEI	Technical Equipment Inspection
TEL	Transporter Erector Launcher
TELINT	Telemetry Intelligence
TEMP	Test and Evaluation Master Plan
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TF	Training Facility
THAAD	Theater High Altitude Air Defense

THREATCON	Threat Condition
TIA	Transparency in Armaments Agreement
TIARA	Tactical Intelligence and Related Activities
TID	Tamper Indicating Device
TIMS	Treaty Information Management System
TISS	Telecommunications and Automated Information Systems Security
TJAG	The Judge Advocate General
TL	Training Launcher
TLC	Training Launch Canister
TLE	Treaty-Limited Equipment
TLI	Treaty-Limited Item
TM	Technical Manual
TM	Treaty Manager
TMD	Theater Missile Defense
TMDE	Test, Measurement, and Diagnostic Equipment
TMO	Technology Management Office
TMO	Treaty Management Office
TMOM	Training Model of a Missile
TNS	Telephone Notification System
TOC	Treaty Operations Center
TOPS	Transportable Operational Planning System
TP	Transportation Plan
TPC	Two-Person Control

TPDC	Training and Professional Development Committee
TPI	Two-Person Integrity
TPS	Transportation Protection Service
TRADOC	U.S. Army Training and Doctrine Command
TRANSEC	Transmission Security
TREAS DEPT	Department of the Treasury
TRQ	Transient Electromagnetic Pulse Emanation Standard (TEMPEST) Requirements Questionnaire
TS	Technical Secretariat
TS	TOP SECRET
TSA	Transportation Security Administration
T-SAPF	Tactical Special Access Program Facility
TSC	Triple-Standard Concertina
T-SCIF	Tactical Sensitive Compartmental Information Facility
TSCM	Technical Surveillance Countermeasures
TSCO	TOP SECRET Control Officer
TSEC	Telecommunications Security
TSG	Telephone Security Group
TSWA	Temporary Secure Working Area
TT	Technology Transfer
TTBT	Threshold Test-Ban Treaty
TTCP	Technology Transfer Control Plan
TTRA	Technology Targeting Risk Assessment

U

U	Unclassified
U.S.	United States
U.S.C.	United States Code
UA	User Agency
UAA	Uncontrolled Access Area
UCMJ	Uniform Code of Military Justice
UCNI	Unclassified Controlled Nuclear Information
UD	Unauthorized Disclosure
UDOC	Unscheduled Discrete Organic Chemical
UIC	Unit Identification Code
UK	United Kingdom
UL	Underwriter's Laboratory
UN	United Nations
UNGA	United Nations General Assembly
UNMOVIC	United Nations Monitoring, Verification, and Inspection Commission
UNSC	United Nations Security Council
UNSCOM	United Nations Special Commission
UNSECNAV	Under Secretary of the Navy
UNTIA	United Nations Transparency in Armaments
UPS	Uninterruptible Power Supply
USA	United States Army
USACIDC	United States Army Criminal Investigation Division Command

USACIDU United States Army Criminal Investigation Command
USAF United States Air Force
USAINSCOM United States Army Intelligence and Security Command
USAMI United States Army Military Intelligence
USASMDC United States Army Space and Missile Defense Command
US-CERT United States Computer Emergency Readiness Team
USCG United States Coast Guard
USCYBERCOM United States Cyber Command
USD(A&T) Under Secretary of Defense (Acquisition and Technology)
USD(AT&L) Under Secretary of Defense (Acquisition, Technology, and Logistics)
USD(I) Under Secretary of Defense (Intelligence)
USD(P) Under Secretary of Defense (Policy)
USDA United States Department of Agriculture
USERID User Identification
USERRA Uniformed Services Employment and Reemployment Rights Act
USG United States Government
USMC United States Marine Corps
USML United States Munitions List
USN United States Navy
USNA United States National Authority
USPS United States Postal Service

USSAN United States Security Authority/North Atlantic Treaty Organization (NATO)
USSID United States Signals Intelligence Directive
USSS United States Secret Service
USSTRATCOM United States Strategic Command
USTR Office of the United States Trade Representative
UXO Unexploded Ordnance

V

VA Department of Veterans Affairs
VA Vulnerability Assessment
VAL Visitor Authorization Letter
VAR Visit Authorization Request
VCC Verification Coordinating Committee
VCJCS Vice Chairman of the Joint Chiefs of Staff
VD Vienna Document
VEREX Verification Experts
VM Volatile Memory

W

WAN Wide Area Network
WBPA Whistleblower Protection Act
WHCA White House Communications Agency
WHG Western Group of Forces
WHO World Health Organization
WHS Washington Headquarters Service

WINPAC	Weapons, Intelligence, Nonproliferation, and Arms Control
WMD	Weapons of Mass Destruction
WNRC	Washington National Records Center
WORM	Write-Once, Read Many
WSA	Weapons Storage Area
XMP	X-Ray and Manipulation Proof
XNAC	Expanded National Agency Check

Y

(No content)

Z

(No content)

Center for Development of Security Excellence

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.